

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

This Page Blank (uspto)

INFORMATION DELIVERY METHOD AND SYSTEM UTILIZING ZERO INTELLIGENCE PROOF PROTOCOL

Patent Number: JP8149124
Publication date: 1996-06-07
Inventor(s): KANDA MASASUKI; YAMANAKA KIYOSHI; TAKASHIMA YOICHI
Applicant(s):: NIPPON TELEGR & TELEPH CORP <NTT>
Requested Patent: ☒ JP8149124
Application Number: JP19950047115 19950307
Priority Number(s):
IPC Classification: H04L9/00 ; H04L9/10 ; H04L9/12 ; G06F13/00 ; G09C1/00
EC Classification:
Equivalents:

Abstract

PURPOSE: To provide an information delivery method and system utilizing the zero intelligence proof protocol by which illegal act is surely prevented by processing simultaneously the process of verifying the user, the process of information delivery and the process of recording and managing communication history data when the user requests the delivery of information to an information server.

CONSTITUTION: A card 1 is used for a random number generating means 12 to generate a random number and sends it to an information server via a communication control means 24. The information server uses a verification means 33 to verify the random number. When the verification is successful, the state is recorded in a history management means 34 as a communication history and managed therein. Then all sets of check texts generated by an information division means 32 are sent. The card 1 links all the sets of the check texts recorded in a storage means 14 and copies an information ciphering secret key and transfer the key to a utility means 23 of the user terminal equipment 2. The utility means 23 decodes the ciphering message stored in the storage means 22 to obtain the message.

Data supplied from the **esp@cenet** database - 12

This Page Blank (uspto)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-149124

(43) 公開日 平成8年(1996)6月7日

(51) IntCl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/00				
9/10				
9/12				
G 0 6 F 13/00	3 5 1 Z	7368-5E		
			H 0 4 L 9/00	Z

審査請求 未請求 請求項の数62 O L (全 65 頁) 最終頁に続く

(21) 出願番号 特願平7-47115

(22) 出願日 平成7年(1995)3月7日

(31) 優先権主張番号 特願平6-35797

(32) 優先日 平6(1994)3月7日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平6-213374

(32) 優先日 平6(1994)9月7日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平6-226282

(32) 優先日 平6(1994)9月21日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72) 発明者 神田 雅透
東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

(72) 発明者 山中 喜義
東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

(72) 発明者 高嶋 洋一
東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

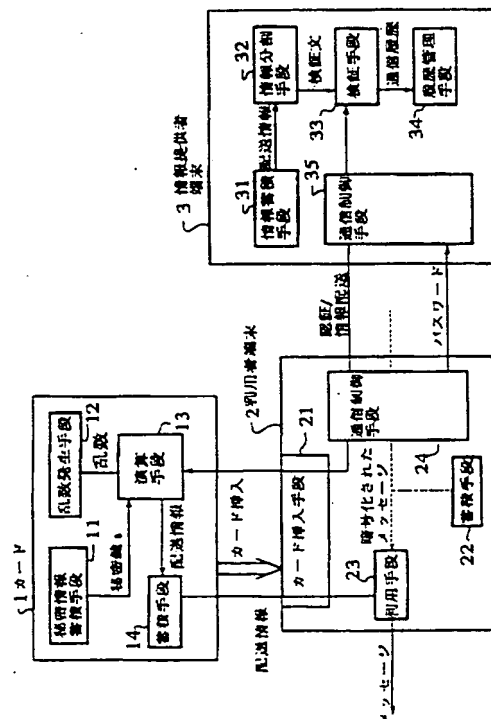
(74) 代理人 弁理士 三好 秀和 (外1名)

(54) 【発明の名称】 ゼロ知識証明プロトコルを利用した情報配送方法およびシステム

(57) 【要約】

【目的】 情報提供者から通信回線により利用者に情報を提供する場合、利用者の正当性と、情報配送の確実性と、配送情報の正当性を保証し、配送情報や受信報告の改竄等の不正行為を防止し、後日これらを証明できる情報配送方法およびシステム。

【構成】 利用者が情報提供者に情報の配送を要求した時に、情報提供者がゼロ知識証明プロトコルにしたがって利用者の利用者認証を行なう過程と、情報提供者が利用者に配送する情報Mをゼロ知識証明プロトコル中における検査文Eに含めて送信し、利用者に情報を1ビットまたは複数ビット単位で配送する過程と、ゼロ知識証明プロトコルの通信履歴データHを情報提供者が記録管理する過程と、を同時に行なう。



【特許請求の範囲】

【請求項1】 少なくとも情報提供者と利用者を含むシステムにおいて、

利用者が情報提供者に情報の配送を要求した時に、
情報提供者が、ゼロ知識証明プロトコルにしたがって利用者の利用者認証を行なう過程と、
情報提供者が、利用者に配送する情報Mをゼロ知識証明プロトコル中における検査文Eに含めて送信し、利用者に情報を1ビットまたは複数ビット単位で配送する過程と、
情報提供者が、ゼロ知識証明プロトコルの通信履歴データHを記録管理する過程と、
を同時に行なうことを特徴とする情報配送方法。

【請求項2】 請求項1に記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、

利用者が、初期応答文Xを情報提供者に送信し、
情報提供者が、利用者に配送する情報Mを利用者に送信し、

利用者が、情報Mを検査文Eとして、初期応答文Xと検査文Eと利用者の秘密情報Sとを用いて応答文Yを作成して情報提供者に送信し、

情報提供者が、情報Mを検査文Eとして、応答文Yは初期応答文Xと検査文Eと利用者の公開情報Iとに対する正しい応答になっているかを検査して、利用者の秘密情報Sを漏らすことなく、利用者は秘密情報Sを知っていることを認証するとともに、利用者は情報Mを確実に受信していることを確認することからなる配送確認プロセスを含むことを特徴とする情報配送方法。

【請求項3】 請求項2に記載の情報配送方法において、
情報提供者から利用者に送信する情報Mについて暗号通信を行なうことを特徴とする情報配送方法。

【請求項4】 請求項3に記載の情報配送方法において、
利用者から情報提供者に送信する初期応答文Xまたは応答文Yの少なくともいずれか一方について暗号通信を行なうことを特徴とする情報配送方法。

【請求項5】 請求項1に記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、

利用者が、初期応答文Xを情報提供者に送信し、
情報提供者が、利用者に配送する情報Mを暗号化した暗号文Cを利用者に送信し、

利用者が、暗号文Cを検査文Eとして、初期応答文Xと検査文Eと利用者の秘密情報Sとを用いて応答文Yを作成して情報提供者に送信し、

情報提供者が、送信した暗号文Cを検査文Eとして、応答文Yは初期応答文Xと検査文Eと利用者の公開情報Iとに対する正しい応答になっているかを検査して、利用

者の秘密情報Sを漏らすことなく、利用者は秘密情報Sを知っていることを認証するとともに、利用者は暗号文Cを確実に受信していることを確認することからなる配送確認プロセスと、

利用者が、暗号文Cを復号して情報Mを獲得することからなる情報取り出しプロセスとを含むことを特徴とする情報配送方法。

【請求項6】 請求項2から請求項5のいずれかに記載の情報配送方法において、

利用者及び情報提供者は、少なくとも情報Mまたは暗号文Cを用いて情報圧縮関数により検査文Eを作成することを特徴とする情報配送方法。

【請求項7】 請求項2から請求項6のいずれかに記載の情報配送方法において、

利用者及び情報提供者は、少なくとも情報Mまたは暗号文Cと初期応答文Xとを用いて一方向性関数により検査文Eを作成することを特徴とする情報配送方法。

【請求項8】 請求項7に記載の情報配送方法において、前記記録管理する過程では、

情報提供者が、少なくとも情報Mまたは暗号文Cと検査文Eと応答文Yとからなる通信履歴データHを記録管理することを特徴とする情報配送方法。

【請求項9】 請求項8に記載の情報配送方法において、更に、

情報提供者が、調停者に対し通信履歴データHを提示し、

調停者が、検査文Eと応答文Yと利用者の公開情報Iとから初期応答文Xを計算し、少なくとも初期応答文Xと情報Mまたは暗号文Cとを用いて一方向性関数により検査文Eを作成し、作成した検査文Eは通信履歴データHに含まれる検査文Eと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Mを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。

【請求項10】 請求項2から請求項9のいずれかに記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、

情報提供者が、利用者に送信する情報Mまたは暗号文Cを任意ビット長のサイズの複数個のブロックに分割し、各ブロックごとに独立して繰り返し配送確認プロセスを行なうことを特徴とする情報配送方法。

【請求項11】 請求項1に記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、

利用者が、初期応答文Xを情報提供者に送信し、
情報提供者が、情報暗号化用秘密鍵Wを生成し、利用者に配送する情報Mを情報暗号化用秘密鍵Wを用いて共通鍵暗号方式により暗号化した暗号文Cを利用者に送信し、

利用者が、暗号文Cを受信した後、受信した旨を情報提

供者に通知し、

情報提供者が、少なくとも情報暗号化用秘密鍵Wを用いて検査文Eを生成して利用者に送信し、

利用者が、初期応答文Xと検査文Eと利用者の秘密情報Sとを用いて応答文Yを作成して情報提供者に送信し、
情報提供者が、応答文Yは初期応答文Xと検査文Eと利用者の公開情報Iとに対する正しい応答になっているかを検査して、利用者の秘密情報Sを漏らすことなく、利用者は秘密情報Sを知っていることを認証するとともに、利用者は検査文Eを確実に受信していることを確認することからなる配送確認プロセスと、

利用者が、少なくとも検査文Eを用いて情報暗号化用秘密鍵Wを取り出し、情報暗号化用秘密鍵Wを用いて共通鍵暗号方式により暗号文Cを復号して情報Mを獲得することからなる情報取り出しプロセスとを含むことを特徴とする情報配送方法。

【請求項12】 請求項11に記載の情報配送方法において、

情報提供者は、少なくとも初期応答文Xと乱数文Zを用いて一方方向性関数により情報暗号化用秘密鍵Wを生成することを特徴とする情報配送方法。

【請求項13】 請求項12に記載の情報配送方法において、前記記録管理する過程では、

情報提供者が、少なくとも乱数文Zと検査文Eと応答文Yとからなる通信履歴データHを記録管理することの特徴とする情報配送方法。

【請求項14】 請求項13に記載の情報配送方法において、更に、

情報提供者が、調停者に対し通信履歴データHを提示し、

調停者が、検査文Eと応答文Yと利用者の公開情報Iとから初期応答文Xを計算し、少なくとも初期応答文Xと乱数文Zを用いて一方方向性関数により情報暗号化用秘密鍵Wを生成し、少なくとも情報暗号化用秘密鍵Wを用いて検査文Eを作成し、作成した検査文Eは通信履歴データHに含まれる検査文Eと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Mを配送したことを認めることからなる過程とを含むことを特徴とする情報配送方法。

【請求項15】 請求項1に記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、

情報提供者が、情報暗号化用秘密鍵Wを生成し、情報Mを情報暗号化用秘密鍵Wを用いて共通鍵暗号方式により暗号化した暗号文Cを利用者に送信し、

利用者が、暗号文Cを受信した後、受信した旨を情報提供者に通知することからなる情報配送プロセスと、

利用者が、初期応答文Xを情報提供者に送信し、
情報提供者が、少なくとも情報暗号化秘密鍵Wを用いて検査文Eを作成して利用者に送信し、

利用者が、初期応答文Xと検査文Eと利用者の秘密情報Sとを用いて応答文Yを作成して情報提供者に送信し、
情報提供者が、応答文Yは初期応答文Xと検査文Eと利用者の公開情報Iとに対する正しい応答になっているかを検査して、利用者の秘密情報Sを漏らすことなく、利用者は秘密情報Sを知っていることを認証するとともに、利用者は検査文Eを確実に受信していることを確認することからなる配送確認プロセスと、

利用者が、少なくとも検査文Eを用いて情報暗号化用秘密鍵Wを獲得し、情報暗号化用秘密鍵Wを用いて共通鍵暗号方式により暗号文Cを復号して情報Mを獲得することからなる情報取り出しプロセスとを含むことを特徴とする情報配送方法。

【請求項16】 請求項15に記載の情報配送方法において、

情報提供者は少なくとも自ら生成した乱数文Zを用いて一方方向性関数により情報暗号化用秘密鍵Wを生成することを特徴とする情報配送方法。

【請求項17】 請求項16に記載の情報配送方法において、

前記配送確認プロセスでは、情報提供者は少なくとも初期応答文Xを用いて一方方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも情報暗号化用秘密鍵Wと鍵暗号化用秘密鍵Kとを用いて検査文Eを生成して利用者に送信し、

前記情報取り出しプロセスでは、利用者は少なくとも初期応答文Xを用いて一方方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも検査文Eと鍵暗号化用秘密鍵Kとを用いて情報暗号化用秘密鍵Wを取り出すことを特徴とする情報配送方法。

【請求項18】 請求項17に記載の情報配送方法において、前記記録管理する過程では、

情報提供者が、少なくとも乱数文Zと検査文Eと応答文Yとからなる通信履歴データHを記録管理することの特徴とする情報配送方法。

【請求項19】 請求項18に記載の情報配送方法において、更に、

情報提供者が調停者に対し通信履歴データHを提示し、
調停者が検査文Eと応答文Yと利用者の公開情報Iとから初期応答文Xを計算し、少なくとも初期応答文Xを用いて一方方向性関数により鍵暗号用秘密鍵Kを、また少なくとも乱数文Zを用いて一方方向性関数により情報暗号化用秘密鍵Wをそれぞれ生成し、少なくとも鍵暗号用秘密鍵Kと情報暗号化用秘密鍵Wとを用いて検査文Eを作成し、作成した検査文Eは通信履歴データHに含まれる検査文Eと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Mを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。

【請求項20】 請求項16に記載の情報配送方法にお

いて、

前記配送確認プロセスでは、情報提供者は少なくとも初期応答文Xおよび利用者と情報提供者が秘密に共有している秘密情報CSとを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも情報暗号化用秘密鍵Wと鍵暗号化用秘密鍵Kとを用いて検査文Eを生成して利用者に送信し、

前記情報取り出しプロセスでは、利用者は少なくとも初期応答文Xと秘密情報CSとを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも検査文Eと鍵暗号化用秘密鍵Kとを用いて情報暗号化用秘密鍵Wを取り出すことを特徴とする情報配送方法。

【請求項21】 請求項20に記載の情報配送方法において、前記記録管理する過程では、

情報提供者が、少なくとも利用者と情報提供者が秘密に共有している秘密情報CSと乱数文Zと検査文Eと応答文Yとからなる通信履歴データHを記録管理することを特徴とする情報配送方法。

【請求項22】 請求項21に記載の情報配送方法において、更に、

情報提供者が調停者に対し通信履歴データHを提示し、調停者が検査文Eと応答文Yと利用者の公開情報Iとから初期応答文Xを計算し、少なくとも初期応答文Xおよび利用者と情報提供者が秘密に共有している秘密情報CSとを用いて一方向性関数により鍵暗号用秘密鍵Kを、また少なくとも乱数文Zを用いて一方向性関数により情報暗号化用秘密鍵Wをそれぞれ生成し、少なくとも鍵暗号用秘密鍵Kと情報暗号化用秘密鍵Wとを用いて検査文Eを作成し、作成した検査文Eは通信履歴データHに含まれる検査文Eと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Mを配送したことを認めることから成る過程を含むことを特徴とする情報配送方法。

【請求項23】 請求項15に記載の情報配送方法において、

利用者は、要求文Rを情報提供者に送信し、情報提供者は、少なくとも要求文Rと自ら生成した乱数文Zとを用いて一方向性関数により情報暗号化用秘密鍵Wを生成することを特徴とする情報配送方法。

【請求項24】 請求項23に記載の情報配送方法において、

利用者から情報提供者に送信する要求文Rについて暗号通信を行なうことを特徴とする情報配送方法。

【請求項25】 請求項23または請求項24に記載の情報配送方法において、

前記配送確認プロセスでは、情報提供者が、少なくとも初期応答文Xを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも情報暗号化用秘密鍵Wと鍵暗号化用秘密鍵Kとを用いて検査文Eを生成して利用者に送信し、

前記情報取り出しプロセスでは、利用者が、少なくとも初期応答文Xを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも検査文Eと鍵暗号化用秘密鍵Kとを用いて情報暗号化用秘密鍵Wを取り出すことを特徴とする情報配送方法。

【請求項26】 請求項25に記載の情報配送方法において、前記記録管理する過程では、

情報提供者が、少なくとも乱数文Zと検査文Eと応答文Yと要求文Rとからなる通信履歴データHを記録管理することを特徴とする情報配送方法。

【請求項27】 請求項26に記載の情報配送方法において、更に、

情報提供者が、調停者に対し通信履歴データHを提示し、

調停者が、検査文Eと応答文Yと利用者の公開情報Iとから初期応答文Xを計算し、少なくとも初期応答文Xを用いて一方向性関数により鍵暗号用秘密鍵Kを、また少なくとも乱数文Zと要求文Rとを用いて一方向性関数により情報暗号化用秘密鍵Wをそれぞれ生成し、少なくとも鍵暗号用秘密鍵Kと情報暗号化用秘密鍵Wとを用いて検査文Eを作成し、作成した検査文Eは通信履歴データHに含まれる検査文Eと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Mを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。

【請求項28】 請求項23または請求項24に記載の情報配送方法において、

前記配送確認プロセスでは、情報提供者が、少なくとも初期応答文Xおよび利用者と情報提供者が秘密に共有している秘密情報CSとを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも情報暗号化用秘密鍵Wと鍵暗号化用秘密鍵Kとを用いて検査文Eを生成して利用者に送信し、

前記情報取り出しプロセスでは、利用者が、少なくとも初期応答文Xと秘密情報CSとを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも検査文Eと鍵暗号化用秘密鍵Kとを用いて情報暗号化用秘密鍵Wを取り出すことを特徴とする情報配送方法。

【請求項29】 請求項28に記載の情報配送方法において、前記記録管理する過程では、

情報提供者が、少なくとも利用者と情報提供者が秘密に共有している秘密情報CSと乱数文Zと検査文Eと応答文Yと要求文Rとからなる通信履歴データHを記録管理することを特徴とする情報配送方法。

【請求項30】 請求項29に記載の情報配送方法において、更に、

情報提供者が、調停者に対し通信履歴データHを提示し、

調停者が、検査文Eと応答文Yと利用者の公開情報Iとから初期応答文Xを計算し、少なくとも初期応答文Xお

よび利用者と情報提供者が秘密に共有している秘密情報CSとを用いて一方向性関数により鍵暗号用秘密鍵Kを、また少なくとも乱数文Zと要求文Rとを用いて一方向性関数により情報暗号化用秘密鍵Wをそれぞれ生成し、少なくとも鍵暗号用秘密鍵Kと情報暗号化用秘密鍵Wとを用いて検査文Eを作成し、作成した検査文Eは通信履歴データHに含まれる検査文Eと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Mを配送したことを認めることから成る過程を含むことを特徴とする情報配送方法。

【請求項31】 請求項15に記載の情報配送方法において、更に、

情報提供者が、利用者には復号できない方式で暗号化した情報暗号化用秘密鍵CWを利用者に送信し、利用者が、暗号化された情報暗号化用秘密鍵CWにデジタル署名した署名付き情報暗号用秘密鍵SWを情報提供者に送信し、

情報提供者が、署名付き情報暗号用秘密鍵SWの署名は正しいかを検証することからなる過程を含むことを特徴とする情報配送方法。

【請求項32】 請求項31に記載の情報配送方法において、

前記配送確認プロセスでは、情報提供者が、少なくとも初期応答文Xを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも情報暗号化用秘密鍵Wと鍵暗号化用秘密鍵Kとを用いて検査文Eを生成して利用者に送信し、

前記情報取り出しプロセスでは、利用者が、少なくとも初期応答文Xを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも検査文Eと鍵暗号化用秘密鍵Kとを用いて情報暗号化用秘密鍵Wを取り出すことを特徴とする情報配送方法。

【請求項33】 請求項32に記載の情報配送方法において、前記記録管理する過程では、情報提供者が、少なくとも情報暗号用秘密鍵Wと署名付き情報暗号用秘密鍵SWと検査文Eと応答文Yとからなる通信履歴データHを記録管理することを特徴とする情報配送方法。

【請求項34】 請求項33に記載の情報配送方法において、更に、

情報提供者が、調停者に対し通信履歴データHを提示し、調停者が、署名付き情報暗号用秘密鍵SWは情報暗号用秘密鍵Wに対する正しい署名であるかどうかを検証した後、検査文Eと応答文Yと利用者の公開情報Iとから初期応答文Xを計算し、少なくとも初期応答文Xを用いて一方向性関数により鍵暗号用秘密鍵Kを生成し、少なくとも鍵暗号用秘密鍵Kと情報暗号化用秘密鍵Wとを用いて検査文Eを作成し、作成した検査文Eは通信履歴データHに含まれる検査文Eと一致するかを検査して、一致

すれば情報提供者は利用者を認証し、かつ利用者に対して情報Mを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。

【請求項35】 請求項31に記載の情報配送方法において、

前記配送確認プロセスでは、情報提供者は少なくとも初期応答文X及び利用者と情報提供者が秘密に共有している秘密情報CSを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも情報暗号化用秘密鍵Wと鍵暗号化用秘密鍵Kとを用いて検査文Eを生成して利用者に送信し、

前記情報取り出しプロセスでは、利用者は少なくとも初期応答文X及び利用者と情報提供者が秘密に共有している秘密情報CSを用いて一方向性関数により鍵暗号化用秘密鍵Kを生成し、少なくとも検査文Eと鍵暗号化用秘密鍵Kとを用いて情報暗号化用秘密鍵Wを取り出すことを特徴とする情報配送方法。

【請求項36】 請求項35に記載の情報配送方法において、前記記録管理する過程では、

情報提供者が、少なくとも情報暗号用秘密鍵Wと署名付き情報暗号用秘密鍵SWと検査文Eと応答文Y及び利用者と情報提供者が秘密に共有している秘密情報CSとからなる通信履歴データHを記録管理することを特徴とする情報配送方法。

【請求項37】 請求項36に記載の情報配送方法において、更に、

情報提供者が調停者に対し通信履歴データHを提示し、調停者が署名付き情報暗号用秘密鍵SWは情報暗号用秘密鍵Wに対する正しい署名であるかどうかを検証した後、検査文Eと応答文Yと利用者の公開情報Iとから初期応答文Xを計算し、少なくとも初期応答文X及び利用者と情報提供者が秘密に共有している秘密情報CSを用いて一方向性関数により鍵暗号用秘密鍵Kを生成し、少なくとも鍵暗号用秘密鍵Kと情報暗号化用秘密鍵Wとを用いて検査文Eを作成し、作成した検査文Eは通信履歴データHに含まれる検査文Eと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Mを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。

【請求項38】 請求項11から請求項37のいずれかに記載の情報配送方法において、

情報提供者から利用者に送信する検査文Eについて暗号通信を行なうことを特徴とする情報配送方法。

【請求項39】 請求項38の情報配送方法において、利用者から情報提供者に送信する初期応答文Xまたは応答文Yの少なくとも一方を暗号通信を行なうことを特徴とする情報配送方法。

【請求項40】 請求項11から請求項37のいずれかに記載の情報配送方法において、

前記配送確認プロセスでは、情報提供者が、少なくとも

検査文 E を暗号化して利用者に送信し、
前記情報取り出しプロセスでは、利用者が、検査文 E を
復号することを特徴とする情報配送方法。

【請求項 4 1】 請求項 1 1 から請求項 4 0 のいずれかに
記載の情報配送方法において、前記利用者認証を行な
う過程及び前記配送する過程は、

検査文 E を任意ビット長のサイズの複数のブロックに
分割し、各ブロックごとに独立して繰り返し配送確認プ
ロセスを行なうことを特徴とする情報配送方法。

【請求項 4 2】 請求項 1 から請求項 4 1 のいずれかに
記載の情報配送方法において、
利用者側の動作は携帯可能な利用者のカードによって実
行されることを特徴とする情報配送方法。

【請求項 4 3】 請求項 1 から請求項 4 2 のいずれかに
記載の情報配送方法において、更に、
前記形態可能な利用者のカードに利用者が受信した情報
M または情報暗号用秘密鍵 W を記録することを含むこと
を特徴とする情報配送方法。

【請求項 4 4】 少なくとも利用者端末と情報提供者端
末とを含むシステムであって、

利用者端末は、
情報提供者端末との間の通信を制御する利用者通信制御
手段と、

利用者が秘密に保持すべき秘密情報を蓄積しておく利用
者秘密情報蓄積手段と、

乱数を発生する乱数発生手段と、

前記利用者通信制御手段を介して通信される初期応答文
と応答文を前記秘密情報と乱数に基づいて生成する利用
者演算手段とを有し、

情報提供者端末は、
利用者端末との間の通信を制御する情報提供者通信制御
手段と、

前記情報提供者通信制御手段を介して利用者に提供する
情報を蓄積しておく情報データベースと、

前記情報提供者通信制御手段を介して利用者の認証を行
なう検証手段とを有することを特徴とする情報配送シス
テム。

【請求項 4 5】 請求項 4 4 に記載の情報配送システム
において、

利用者端末は更に前記利用者通信制御手段を介して情報
提供者から配送された情報を蓄積する情報蓄積手段を有
することを特徴とする情報配送システム。

【請求項 4 6】 請求項 4 4 または請求項 4 5 に記載の
情報配送システムにおいて、

利用者端末および情報提供者端末の双方が更に共通鍵暗
号方式または公開鍵暗号方式、もしくはその両方の暗号
方式による暗号通信を行う暗号手段を有することを特徴
とする情報配送システム。

【請求項 4 7】 請求項 4 6 に記載の情報配送システム
において、

情報提供者端末は更に前記暗号手段で利用される情報提
供者が秘密に保持すべき情報を蓄積する情報提供者秘密
情報蓄積手段を有することを特徴とする情報配送システ
ム。

【請求項 4 8】 請求項 4 4 から請求項 4 7 のいずれかに
記載の情報配送システムにおいて、

利用者端末の前記利用者演算手段および情報提供者端末
の前記検証手段の双方が情報圧縮関数または一方向性関
数、もしくはその両方の関数による関数演算を行う手段
を有することを特徴とする情報配送システム。

【請求項 4 9】 請求項 4 4 から請求項 4 8 のいずれかに
記載の情報配送システムにおいて、

情報提供者端末は更に通信履歴データを記録管理する通
信履歴ファイルを有することを特徴とする情報配送シス
テム。

【請求項 5 0】 請求項 4 9 に記載の情報配送システム
において、更に、

情報提供者が利用者に情報を提供したことを照明する通
信履歴データについて、通信履歴データの正当性を検査
する調停端末であって、

初期応答文と検査文を生成する調停演算手段と、

通信履歴データ中の検査文と前記調停演算手段で生成し
た検査文とに基づいて該通信履歴データの正当性を検査
する調停検証手段とを有するものを含むことを特徴とす
る情報配送システム。

【請求項 5 1】 請求項 4 4 から請求項 5 0 のいずれかに
記載の情報配送システムにおいて、

情報提供者端末は更に前記情報提供者通信制御手段を介
して利用者へ配送する情報を任意ビット長サイズの複数
のブロックに分割する情報分割手段を有し、

利用者端末は更に前記複数のブロックに分割された情
報を元の情報に再構成する情報再構成手段を有すること
を特徴とする情報配送システム。

【請求項 5 2】 少なくとも利用者端末と情報提供者端
末とを含むシステムであって、

利用者端末は、
情報提供者端末との間の通信を制御する利用者通信制御
手段と、

利用者が秘密に保持すべき秘密情報を蓄積しておく利用
者秘密情報蓄積手段と、

前記利用者通信制御手段を介して情報提供者端末との間
で暗号通信を行う利用者共通鍵暗号手段と、

乱数を発生する乱数発生手段と、

前記利用者通信制御手段を介して通信される初期応答文
と応答文と秘密鍵を生成する利用者演算手段と、

前記利用者通信制御手段を介して情報提供者から配送さ
れた情報を蓄積する情報蓄積手段とを有し、

情報提供者端末は、

利用者端末との間の通信を制御する情報提供者通信制御
手段と、

前記情報提供者通信制御手段を介して利用者に提供する情報を蓄積しておく情報データベースと、
秘密鍵と検査文を生成する情報提供者演算手段と、
前記情報提供者通信制御手段を介して利用者端末との間で暗号通信を行う情報提供者共通鍵暗号手段と、
前記情報提供者通信制御手段を介して利用者の認証を行なう検証手段とを有することを特徴とする情報配送システム。

【請求項53】 請求項52に記載の情報配送システムにおいて、

情報提供者端末は更に前記情報提供者演算手段で利用される乱数を発生する乱数発生手段を有することを特徴とする情報配送システム。

【請求項54】 請求項52または請求項53に記載の情報配送システムにおいて、

利用者端末および情報提供者端末の双方が更に公開鍵暗号方式による暗号通信を行なう公開鍵暗号手段を有することを特徴とする情報配送システム。

【請求項55】 請求項52から請求項54のいずれかに記載の情報配送システムにおいて、

情報提供者端末は更に前記情報提供者演算手段または前記公開鍵暗号手段で利用される情報提供者が秘密に保持すべき情報を蓄積する情報提供者秘密情報蓄積手段を有することを特徴とする情報配送システム。

【請求項56】 請求項52から請求項55のいずれかに記載の情報配送システムにおいて、

利用者端末は更にデジタル署名を行うデジタル署名手段を有し、
情報提供者端末はデジタル署名を検証するためのデジタル署名検証手段を有することを特徴とする情報配送システム。

【請求項57】 請求項52から請求項56のいずれかに記載の情報配送システムにおいて、

情報提供者端末は更に通信履歴データを記録管理する通信履歴ファイルを有することを特徴とする情報配送システム。

【請求項58】 請求項57に記載の情報配送システムにおいて、更に、

情報提供者が利用者に情報を提供したことを証明する通信履歴データについて、通信履歴データの正当性を検査する調停端末であって、

初期応答文と秘密鍵と検査文を生成する調停演算手段と、

通信履歴データ中の検査文と前記調停演算手段で生成した検査文とに基づいて該通信履歴データの正当性を検査する調停検証手段とを有するものを含むことを特徴とする情報配送システム。

【請求項59】 請求項58に記載の情報配送システムにおいて、

調停端末が更に通信履歴データ中の署名付き情報暗号用

秘密鍵の署名は正当であることを検証する検証手段を有することを特徴とする情報配送システム。

【請求項60】 請求項52から請求項59のいずれかに記載の情報配送システムにおいて、

情報提供者端末は更に前記情報提供者通信制御手段を介して利用者へ配送する情報を任意ビット長サイズの複数のブロックに分割する情報分割手段を有し、

利用者端末は更に前記複数のブロックに分割された情報を元の情報に再構成する情報再構成手段を有することを特徴とする情報配送システム。

【請求項61】 請求項44から請求項60のいずれかに記載の情報配送システムにおいて、

利用者端末は前記利用者秘密鍵蓄積手段、乱数発生手段、利用者演算手段を含んだカードと、

該カードが挿入されるカード挿入手段とを有することを特徴とする情報配送システム。

【請求項62】 請求項61に記載の情報配送システムにおいて、

前記カードは更に情報提供者から配送された情報を蓄積する情報カード蓄積手段を有することを特徴とする情報配送システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、電気通信システムを用いて利用者が要求した情報を情報提供者が提供する場合に、情報提供者が利用者認証により利用者の正当性を認証しつつ、かつ利用者に要求された情報を利用者まで確実に配送するとともに、後日利用者から要求した情報を受信していないなどの異議申し立てに対して、情報提供者が間違いなく要求された情報を利用者に配送し、かつ利用者が受信している事実を証明できるようにするためのものであり、特に有料情報提供サービスや配達証明サービスなどに有用な情報配送方法およびシステムに関する。

【0002】

【従来の技術】 従来、代表的な認証方法としてはシステム利用者の正当性を検査する利用者認証方式と、情報が正当なものであることを証明するメッセージ認証方式と、更にこれらを組み合わせて作成した情報が正当なものであることを情報作成者が保証するデジタル署名方式がある。ここで、簡単に利用者認証方式とメッセージ認証方式とデジタル署名方式について、それぞれ図を参照しながら説明する。

【0003】 図1(a)は利用者認証方式の代表的な例であるFiat Shamir 法 (A.Fiat and A.Shamir: "How to prove yourself, practical solutions to identification and signature problems", Proc. of Crypto' 86, 1986.5並びに米国特許第4,748,668号) による認証方式の概念図である。

【0004】 このFiat Shamir 法によれば、秘密情報 s

を所有している者（以下、証明者という）が検証者に対してその正当性を証明しようとしたとき、 $N (=pq : p, q \text{ は互いに異なる大きな素数})$ と $I (=s^2 \pmod{N})$ を証明者の公開情報とし、 s と p, q を証明者の秘密情報として以下のように認証される。

【0005】まず始めに証明者が乱数 R を生成させ、初期応答文 $X = R^2 \pmod{N}$ を計算し、検証者に X を送る。前記 X を受信した検証者は検査文 e としてランダムに 0 または 1 を選び、証明者に e を送る。前記 e を受信した証明者は、応答文 $Y = R s^e \pmod{N}$ を計算し、検証者に Y を送る。前記 Y を受信した検証者は、検証式 $Y^2 = X \times I^e \pmod{N}$ が成立するかを検証する。

【0006】ここまでを 1 ラウンドとして、これを t ラウンド繰り返すことにより、秘密情報 s を知らない第三者が検証者の検証式をクリアできる確率は $(1/2^t)$ となる。したがって、十分に大きな t において正常に認証が終了した場合、検証者は検証相手（証明者）を秘密情報 s を所有している正当な証明者であると判断して構わない。

【0007】なお、この認証方式は一般にゼロ知識証明に基づく認証方式と呼ばれ、証明者は検証者に対して秘密情報 s を所有している事実だけを伝え、秘密情報 s に関するその他の内容は一切漏らさないというメリットがある。

【0008】しかし、Fiat Shamir 法では証明者と検証者との通信履歴が、後日検証者が証明者を認証したことの証拠にならないという問題があった。そのため、この問題に対する解決方法としては桜井（特開平5-12321号）による認証方式が提案されている。この認証方式によれば、検証者が証明者を認証した後でも検証者が証明者を本当に認証したことの証拠が残るとされている。

【0009】しかし、ここで証拠として残るのはあくまで検証者が証明者を通信を介して認証したという事実についてのみであり、この認証事実の他は通信内容を始めとしてどのような通信が行われたのかについて何ら言及するものではない。また、認証事実の証拠として通信系列全てを記録保管するため、検証者が記録保管しておかなければならない情報量が多いという欠点もある。

【0010】次に、図1(b)は、メッセージ認証の一例である認証子法による認証方式の概念図である。この認証方式によれば、メッセージ M を送信したい証明者は秘密鍵 K_h をパラメータとするハッシュ関数 h を利用してメッセージ M に対する認証子 $h_k(M)$ を作成し、前記メッセージ M と共に前記認証子を送信相手である検証者に送信する。検証者はあらかじめ証明者と同じ秘密鍵 K_h を秘密裏に共有しているので、受信したメッセージから上記と同じように秘密鍵 K_h を用いて認証子を作成し、受信した認証子と照合検査する。この照合に成功すれば、受信したメッセージの正当性が保証される。これ

は秘密鍵 K_h を知らなければ、任意のメッセージに対する正しい認証子は作成できないためである。

【0011】しかし、上記の利用者認証、メッセージ認証は共に、基本的には第三者による不正行為を防止することが最大の目的であり、前記利用者認証が正常に終了したことで保証されるのは、あくまで証明者が正当な秘密情報の所有者であること、すなわち第三者が不正に利用していないということだけであり、また前記メッセージ認証において照合検査に成功したことで保証されるのは、第三者によるメッセージの改竄などの不正行為が行われていないということだけである。したがって、上記の2つの認証方式は共に、基本的には第三者の不正行為に対してのみ有効であり、証明者もしくは検証者による不正行為に対してはまるで効力を持たないのが欠点である。

【0012】次に、図1(c)はデジタル署名の一例であるRSA署名法(R.L.Rivest, A.Shamir, L.Adleman, "A method for obtaining digital signatures and public-key cryptosystem", Comm. ACM, vol.21, No.2, 1978.2)の概念図である。

【0013】RSA署名法によれば、 e と $N (=pq : p, q \text{ は互いに異なる大きな素数})$ を署名者の公開情報、 $d [e \times d \pmod{(p-1)(q-1)} = 1]$ と p, q を署名者の秘密情報として以下のように認証される。

【0014】まず署名者は、メッセージ M を確かに署名者が作成したものであることを保証するために署名文 $C = M^d \pmod{N}$ を計算し、 C を検証者に送信する。前記 C を受信した検証者は $M = C^e \pmod{N}$ を計算し、得られたメッセージ M の正当性を判断する。この時、得られたメッセージ M が正当であると判断されれば、受信したメッセージ M が署名者により間違いなく作成されたものであることが保証される。

【0015】これは秘密情報 d を知らなければ任意のメッセージに対する正しい署名文を作成できないためであり、しかも秘密情報 d は各個人固有のもので一人ずつ異なるため、署名者自体も特定されることになるからである。したがって、第三者や検証者がメッセージ内容を改竄したり、あるいは署名者がメッセージ内容を否定したりするなどの不正行為は困難であると考えられている。

【0016】しかし、これはあくまでメッセージのやり取りが正常に終了した時点以後から効力が生じるものであり、それ以前、すなわち署名者からみて送信した署名文 C が確実に検証者に届いているかどうかの保証は何もないため、検証者に署名文 C を受信していないと主張されてしまえば、署名者にはその主張に対抗する手段がないのが欠点である。

【0017】

【発明が解決しようとする課題】利用者が要求した情報を情報提供者が提供する場合には以下の4条件、すなわち、(1) 正当な利用者であることを保証する利用者認

証、(2) 情報提供者は利用者が要求した情報を確実に提供し、かつ利用者が提供された情報を受信したことを保証する配送証明、(3) 提供した情報が正当なものであり、改竄などの不正行為を防止できる内容証明、

(4) 後日、必要に応じて情報提供者が調停者に通信履歴などの証拠を提示することにより(1)~(3)のすべてについて証明できること、を満たすことが必要である。

【0018】しかし、従来方式で説明したようにFiat Shamir 法では(1)のみ、桜井(特開平5-12321号)の方式では(1)と(4)の一部(利用者認証の証拠のみ)、メッセージ証拠では(3)の一部のみ(情報が正当である保証のみ)、RSA署名法では(3)のみが満たされるだけであるため、ある種の不正行為、特に(2)のように利用者が提供された情報を受信しているにもかかわらず、受信していないというような不当な主張に対して、情報提供者は全く対抗できないという欠点がある。

【0019】本発明の目的は、情報提供者から利用者(カード、利用者端末等を含む)に対して必要なメッセージを送信する場合に、従来方式では満たせなかった上記の4条件すべてを満たすことができるゼロ知識証明プロトコルを利用した情報配送方法およびシステムを提供することである。

【0020】

【課題を解決するための手段】本発明の一側面によると、少なくとも情報提供者と利用者を含むシステムにおいて、利用者が情報提供者に情報の配送を要求した時に、情報提供者が、ゼロ知識証明プロトコルにしたがって利用者の利用者認証を行なう過程と、情報提供者が利用者に配送する情報Mをゼロ知識証明プロトコル中における検査文Eに含めて送信し、利用者に情報を1ビットまたは複数ビット単位で配送する過程と、情報提供者が、ゼロ知識証明プロトコルの通信履歴データHを記録管理する過程とを同時に行なうことを特徴とする情報配送方法が提供される。

【0021】また、本発明の他の側面によると、少なくとも利用者端末と情報提供者端末とを含むシステムであって、利用者端末は、情報提供者端末との間の通信を制御する利用者通信制御手段と、利用者が秘密に保持すべき秘密情報を蓄積しておく利用者秘密情報蓄積手段と、乱数を発生する乱数発生手段と、前記利用者通信制御手段を介して通信される初期応答文と応答文を前記秘密情報と乱数に基づいて生成する利用者演算手段とを有し、情報提供者端末は、利用者端末との間の通信を制御する情報提供者通信制御手段と、前記情報提供者通信制御手段を介して利用者に提供する情報を蓄積しておく情報データベースと、前記情報提供者通信制御手段を介して利用者の認証を行なう検証手段とを有することを特徴とする情報配送システムが提供される。

【0022】また、本発明の他の側面によると、少なくとも利用者端末と情報提供者端末とを含むシステムであって、利用者端末は、情報提供者端末との間の通信を制御する利用者通信制御手段と、利用者が秘密に保持すべき秘密情報を蓄積しておく利用者秘密情報蓄積手段と、前記利用者通信制御手段を介して情報提供者端末との間で暗号通信を行う利用者共通鍵暗号手段と、乱数を発生する乱数発生手段と、前記利用者通信制御手段を介して送信される初期応答文と応答文と秘密鍵を生成する利用者演算手段と、前記利用者通信制御手段を介して情報提供者から配送された情報を蓄積する情報蓄積手段とを有し、情報提供者端末は、利用者端末との間の通信を制御する情報提供者通信制御手段と、前記情報提供者通信制御手段を介して利用者に提供する情報を蓄積しておく情報データベースと、秘密鍵と検査文を生成する情報提供者演算手段と、前記情報提供者通信制御手段を介して利用者端末との間で暗号通信を行なう情報提供者共通鍵暗号手段と、前記情報提供者通信制御手段を介して利用者の認証を行なう検証手段とを有することを特徴とする情報配送システムが提供される。

【0023】

【作用】本発明によれば、第一に情報提供者による利用者の認証方法としてゼロ知識証明プロトコルを利用しているため、ゼロ知識証明プロトコルの目的や従来からの利用方法からいっても、利用者が正当なカードを利用していなければ情報提供者の検証をクリアし続けることはほとんど不可能であり、認証段階でほぼ完全に拒絶される。

【0024】第二に情報提供者から配送情報を利用者へ配送する部分では、配送情報をゼロ知識証明プロトコルの検査文に含めて配送を行なっているため、ゼロ知識証明プロトコルが正常に終了すれば、カード上において間違いなく検査文、すなわち配送情報を受信・記録し、適正な処理をしていたことになる。また、途中で情報提供者の検証に失敗した場合にはそれ以降の認証は打ち切れ、残りの検査文は配送されないため、利用者が知ることのできる配送情報は検証に失敗する以前のものに限られる。

【0025】第三に通信履歴を記録管理することにより情報提供者と利用者との間で正常な認証が行なわれたことを情報提供者は確認できるので、第二の効果と合わせて利用者は配送情報を受信し、かつカードの蓄積手段に配送情報が記録されているはずである。このことは、情報提供者から開示される通信履歴と利用者から提出されるカードに記録された配送情報とを照合することによって、利用者が情報暗号化用秘密鍵を生成できる状態であるかどうかを判定できる。なお、この場合、利用者からカードの提出がない場合には、情報暗号化用秘密鍵は生成できる状態にあると判定する。

【0026】したがって、不正な利用者がシステムを利

用したり、あるいは配送情報のすべてを不正に搾取したりすることはできない。また、正常に認証が終了しているにも関わらず利用者が配送情報を受信していないなどという不当な主張に対して、情報提供者は通信履歴を開示するとともに、利用者にカードを提出するよう要求することにより対抗できる。

【0027】

【実施例】以下、本発明の実施例を図面を用いて説明する。

【0028】図2は、本発明の第1実施例における情報配送システムの構成例を示す図である。図2において、1は利用者が所有するカードであり、11はカード固有の秘密情報を蓄積する秘密情報蓄積手段、12はゼロ知識証明プロトコルで利用する乱数発生手段、13はプロトコルを実行するうえで必要な演算を行う演算手段、14は情報提供者からの情報を記録する蓄積手段である。なお、これらの手段はいずれもIC等の耐タンパー装置上に組み込まれており、物理的に安全である。

【0029】2は利用者が使用する固定型の利用者端末であり、21はカード挿入手段、22は情報提供者からの情報を蓄積する蓄積手段、23は情報を利用する利用手段、24は情報提供者との間で通信を行なうための通信制御手段である。

【0030】3は利用者に配送情報の配送する情報提供者端末であり、31は配送情報を蓄積する情報蓄積手段、32は配送情報を分割して検査文の組を作成する情報分割手段、33はゼロ知識証明プロトコルの検証を行なう検証手段、34は通信履歴や認証記録を記録管理しておく履歴管理手段、35は利用者端末との間で通信を行うための通信制御手段である。

【0031】次に、図2のシステムにおけるゼロ知識証明プロトコルを利用した情報配送方法について、図3および図4に示す処理フローチャートと配送情報の例を基に説明する。なお、ここではゼロ知識証明プロトコルとしてFiat Shamir法を用いることとし、準備段階として、信頼できるセンタが各利用者ごとに P 、 Q 、 N 、 I 、 s を設定し、このうち N と I を利用者の公開情報として公開し、 s を利用者の秘密情報としてカード1の秘密情報蓄積手段11に蓄積して利用者に配布する。ここで、 P と Q は互いに異なる大きな素数であり、 $N=PQ$ である。また、 $I=s^2 \pmod{N}$ が成立している。

【0032】情報暗号化用秘密鍵 W で暗号化されたメッセージ $W(m)$ をすでに利用者端末2の蓄積手段22に蓄積している利用者に対して、前記情報暗号化用秘密鍵 W を配送情報として配送する場合の例を説明する。

【0033】まず、利用者は、自分のカード1をカード挿入手段21に挿入後、情報提供者に情報暗号化用秘密鍵 W の配送を依頼する。(S1)。

【0034】情報提供者は、情報蓄積手段31に蓄積されている情報暗号化用秘密鍵 W を図4に示す配送情報5

0のように情報分割手段32において g ビットごとに分割し、 g ビットで構成される検査文 e_{ji} の組を作成する(S2)。ここで、情報暗号化用秘密鍵 W のビット数を L とすると、検査文の組は L/g 個作成されることになり、 i は1から g まで、 j は1から L/g までの値をとる。

【0035】次に、カード1は、乱数発生手段12において g 個の乱数 R_i を生成し(S3)、それぞれについて演算手段13において $X_i = R_i^2 \pmod{N}$ を計算し、 X_i を通信制御手段24を経由して情報提供者に送信する(S4)。

【0036】通信制御手段35を経由して X_i を受信した情報提供者は、 j 組目の検査文 e_{ji} を通信制御手段35を経由してカード1に送信する(S5)。

【0037】カード1では、通信制御手段24を経由して受信した検査文 e_{ji} のそれぞれのビット i に対し、演算手段13において0なら $Y_i = R_i$ を、1なら秘密情報蓄積手段11に蓄積されている秘密情報 s を用いて $Y_i = s R_i \pmod{N}$ を計算し、蓄積手段14に検査文 e_{ji} を記録した後、通信制御手段24を経由して Y_i を情報提供者に送信する(S6)。

【0038】情報提供者は、通信制御手段35を経由して受信した前記 X_i と前記 Y_i 、および前記検査文 e_{ji} からそれぞれのビット i に対し、検証手段33において検査ビットが0ならば検証式 $Y_i^2 = X_i \pmod{N}$ を、1ならば検証式 $Y_i^2 = X_i I \pmod{N}$ を満たすかどうかを検証する(S7)。この検証に失敗した場合には、カード1は不正であるとみなして、それ以降の利用を中止(S8)し、成功した場合には前記 X_i と前記 Y_i 、および前記検査文 e_{ji} を通信履歴として履歴管理手段34に記録管理する(S9)。そして、上記S3以降のステップを情報分割手段32で作成した L/g 個の検査文 e_{ji} の組すべてを送信し終わるまで繰り返し(S10)、最終的に情報提供者は、情報分割手段32で作成した L/g 個の検査文 e_{ji} の組すべての送信が終了した時点をもって情報暗号化用秘密鍵 W の配送が終了したとみなす(S11)。

【0039】カード1では蓄積手段14に記録された L/g 個の検査文 e_{ji} の組すべてを結合し、情報暗号化用秘密鍵 W を複製した(S12)後、利用者端末2の利用手段23に転送する(S13)。利用手段23では転送されてきた情報暗号化用秘密鍵 W を用いて蓄積手段22に蓄積されている暗号化されたメッセージ $W(m)$ を復号し、メッセージ m を得ることができる(S14)。

【0040】以上の説明は、利用者に対して確実に必要な情報を配送し、かつ利用者のカードに記録されたことを情報提供者が確認できるものである。例えば、メッセージ m を著作物などの有料情報とした時、情報暗号化用秘密鍵 W で暗号化した $W(m)$ をあらかじめ利用者へ送信し、またはCD-ROM等の媒体に記録して配布して

おき、その後情報提供者が前記情報暗号化用秘密鍵 W を上記の配送方法によって送信することにより、メッセージ m を間違いなく購入した利用者に対して著作権使用料などの情報料を徴収するときに、情報提供者は履歴管理手段34に記録管理された通信履歴を利用できる。また、電子メールにおいて郵便内容 m を情報暗号化用秘密鍵 W で暗号化し、あらかじめ配達先に $W(m)$ を送信しておき、後日電子メール管理者から配達先に対して前記情報暗号化用秘密鍵 W を上記の配送方法により送信することにより、電子メール管理者は電子メールの配達証明に利用できるなど、さまざまな利用が可能である。

【0041】以上説明したとおり、この第1実施例では、第一に情報提供者による利用者の認証方法としてゼロ知識証明プロトコルを利用しているため、ゼロ知識証明プロトコルの目的や従来からの利用方法からいっても、利用者が正当なカードを利用していなければ情報提供者の検証をクリアし続けることはほとんど不可能であり、認証段階でほぼ完全に拒絶される。

【0042】第二に情報提供者から配送情報を利用者へ配送する部分では、配送情報をゼロ知識証明プロトコルの検査文に含めて配送を行なっているため、ゼロ知識証明プロトコルが正常に終了すれば、カード上において間違いなく検査文、すなわち配送情報を受信・記録し、適正な処理をしていたことになる。また、途中で情報提供者の検証に失敗した場合にはそれ以降の認証は打ち切れ、残りの検査文は配送されないため、利用者が知ることのできる配送情報は検証に失敗する以前のものに限られる。

【0043】第三に通信履歴（前記 X_i 、前記 Y_i 、前記検査文 e_{ji} ）を記録管理することにより情報提供者と利用者との間で正常な認証が行なわれたことを情報提供者は確認できるので、第二の効果と合わせて利用者は配送情報を受信し、かつカードの蓄積手段14に配送情報が記録されているはずである。このことは、情報提供者から開示される通信履歴と利用者から提出されるカードに記録された配送情報とを照合することによって、利用者が情報暗号化用秘密鍵 W を生成できる状態であるかどうかを判定できる。なお、この場合、利用者からカードの提出がない場合には、情報暗号化用秘密鍵 W は生成できる状態にあると判定する。

【0044】したがって、不正な利用者がシステムを利用したり、あるいは配送情報のすべてを不正に搾取したりすることはできない。また、正常に認証が終了しているにも関わらず利用者が配送情報を受信していないなどという不当な主張に対して、情報提供者は通信履歴を開示するとともに、利用者にはカードを提出するよう要求することにより対抗できる。

【0045】なお当然のことであるが、上記の実施例においても、配送情報すべてを分割して検査文 e_{ji} を生成する必要はなく、例えば、配送情報の始めから gn ビ

ット目までを検査文 e_{ji} （ $j=1, \dots, n$ ）とし、 n 組の検査文 e_{ji} によるゼロ知識証明プロトコルが終了した後、配送情報の残りの部分を一括して送信するような情報の配送方法も考えられる。この場合、 n の値を様々に変えることにより、ゼロ知識証明におけるセキュリティレベルを変えられるうえ、通信量を削減できるといった特徴がある。例えば n を L/g の半分とすれば、通信量もほぼ半分となる。

【0046】また、検査文 e_{ji} の生成方法についても、単純に配送情報を分割して生成するだけでなく、ダミー情報を付加したり、あるいは暗号化を行ったりして生成することも可能である。この場合、カード内にあらかじめ設定されている秘密情報、もしくは蓄積された検査文 e_{ji} から自律的にダミー情報を除去、あるいは復号を行ったりして元の配送情報に還元する機能を持たせることにより、ゼロ知識証明を正常に終了しないかぎり、前記配送情報を取り出せないようにできる。したがって、第三者もしくは利用者が検査文 e_{ji} を不正に搾取したり、大部分の検査文 e_{ji} を受信した後、故意に認証を失敗させ、検査文 e_{ji} のうち配送されてこなかった残りの部分を予測したりする等の不正行為を行ない、情報提供者が配送に失敗したと判断あるいは気がつかないうちに、第三者もしくは利用者が配送情報を獲得してしまうことがないようにできる。

【0047】なお、上述の第1実施例による情報配送方法およびシステムでは、ゼロ知識証明プロトコルに必要な情報はすべて耐タンパー装置上に組み込まれており、実際の情報配送においても耐タンパー装置上に組み込まれた手段のみを用いて実行されるため、前記情報が外部に漏れることはなく、たとえカード所有者であっても前記情報を知ることができない。したがって、カード自体を偽造したり、あるいはカード上の記録情報を書き換えたりする等の不正行為を防止できる。

【0048】次に本発明の第2実施例について説明する。

【0049】図5は本発明の第2実施例における情報配送システムの構成を示すブロック図であり、10は情報提供者端末20から情報の提供を受ける利用者の端末

（利用者端末）を示し、100は通信回線30を制御する通信制御手段、101は利用者の秘密情報を蓄積しておく利用者秘密情報蓄積手段、102は利用者が必要な情報を一時的に蓄積する一時メモリ、103は利用者が乱数を生成するための乱数発生手段、104は利用者が必要な演算を行う機能を有する演算手段、105は共通鍵暗号方法（例えば、DES、FEAL）による暗号通信を行うための共通鍵暗号手段、106は利用者が受信した情報を出力もしくは利用する情報出力／利用手段である。

【0050】また、20は情報を提供する情報提供者の端末（情報提供者端末）を示し、200は通信回線30

を制御する通信制御手段、201は情報提供者の秘密情報を蓄積しておく情報提供者秘密情報蓄積手段、202は提供する情報が蓄積してある情報データベース、203は情報提供者が必要な情報を一時的に蓄積する一時メモリ、204は情報提供者が必要な演算を行う機能を有する演算手段、205は共通鍵暗号方法による暗号通信を行うための共通鍵暗号手段、206はFiat Shamir 法に基づいて通信系列の正当性を検証する検証手段である。30は利用者と情報提供者とを通信で接続する通信回線を表す。

【0051】以下、図6のフローチャートにしたがって動作手順を説明する。

【0052】まず基準段階として、信頼できるセンタが各利用者ごとに p_1, q_1, I, s を設定し、このうち N_1 と I を利用者の公開情報として公開し、 s を利用者の秘密情報として利用者秘密情報蓄積手段101に蓄積して利用者に秘密裏に配布する。ここで、 p_1 と q_1 はそれぞれ互いに異なる大きな素数であり、 $N_1 = p_1 \times q_1$ である。また、 $I = s^2 \pmod{N_1}$ が成立している。

【0053】さらに、各情報提供者と各利用者の間にはシステム秘密鍵 SK を設定し、利用者秘密情報蓄積手段101および情報提供者秘密情報蓄積手段201に登録しておく。このシステム秘密鍵 SK は、各情報提供者と各利用者の間ごとに異なる方が好ましいことはいうまでもないが、システム設計上、システム全体の共通鍵として1種類あるいは複数種類のシステム秘密鍵を複数の利用者で利用しても構わない。

【0054】(1) 配送確認ステップ

利用者端末10は、乱数発生手段103により g 個の乱数 R_i ($i=1, 2, \dots, g$)を生成し、一時メモリ102に蓄積し(S101)、その後、それぞれの乱数について演算手段104により初期応答文 $X_i = R_i^2 \pmod{N_1}$ ($i=1, 2, \dots, g$)を計算し(S102)、通信回線30を介して情報提供者端末20に送信する(S103)。

【0055】情報提供者端末20は、受信した初期応答文 X_i ($i=1, 2, \dots, g$)を一時メモリ203に蓄積し(S104)、その後、利用者端末10に配送する情報 M を情報データベース202より取り出して(S105)、情報提供者秘密情報蓄積手段201に蓄積されたシステム秘密鍵 SK を秘密鍵として、共通鍵暗号手段205により暗号化した暗号文 $C = E_{SK}(M)$ を通信回線30を介して利用者端末10に送信する(S106)。

【0056】利用者端末10は、受信した暗号文 C を一時メモリ102に蓄積し(S107)、その後、演算手段104において暗号文 C を用いて g ビットの情報圧縮関数であるハッシュ関数 h により検査文 $e_i = h(C)$ ($i=1, 2, \dots, g$)を生成する(S108)。生成

した検査文 e_i のそれぞれのビット i に対し、一時メモリ102に蓄積された乱数 R_i と利用者秘密情報蓄積手段101に蓄積された利用者の秘密情報 s とから $e_i = 0$ ならば $Y_i = R_i$ を、 $e_i = 1$ ならば $Y_i = s R_i \pmod{N_1}$ を計算し(S109)、応答文 Y_i ($i=1, 2, \dots, g$)として情報提供者端末20に通信回線30を介して送信する(S110)。

【0057】情報提供者端末20は、受信した応答文 Y_i ($i=1, 2, \dots, g$)を一時メモリ203に蓄積し(S111)、その後、演算手段204において暗号文 C を用いて g ビットの情報圧縮関数であるハッシュ関数 h により検査文 $e_i = h(C)$ ($i=1, 2, \dots, g$)を生成する(S112)。検証手段206において利用者の公開情報 I および一時メモリ203に蓄積された初期応答文 X_i と応答文 Y_i と検査文 e_i とからそれぞれのビット i に対し、 $e_i = 0$ ならば検証式 $Y_i^2 = X_i \pmod{N_1}$ を、 $e_i = 1$ ならば検証式 $Y_i^2 = X_i \times I \pmod{N_1}$ を満たすかどうかを検証する(S113)。この検証に失敗した場合には利用者は不正であると見做してそれ以降の利用を禁止し(S114A)、成功した場合には情報 M の配送が正常に終了したと判断する(S114B)。

【0058】(2) 情報取り出しステップ

利用者端末1は、一時メモリ102に蓄積された暗号文 C を利用者秘密情報蓄積手段101に蓄積されたシステム秘密鍵 SK を秘密鍵として共通鍵暗号手段105により情報 $M = D_{SK}(C)$ に復号して、情報出力/利用手段106から情報 M を出力する(S115)。

【0059】上記の情報配送方法を用いて配送確認ステップが正常に終了したことは、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文 e_i ($i=1, 2, \dots, g$)が正しく生成されたことの証明となる。また、検査文 e_i ($i=1, 2, \dots, g$)は利用者端末10が受信した暗号文 C より情報圧縮関数であるハッシュ関数を用いて生成されることから、正しい暗号文 C を受信しなければ正しい検査文 e_i ($i=1, 2, \dots, g$)を生成することはできない。したがって、検査文 e_i ($i=1, 2, \dots, g$)を利用者が正しく生成できることと、利用者が暗号文 C (および情報 M)を正常に受信したこととは同値となる。以上の説明から明らかなように、情報提供者は正確かつ確実に情報を利用者に配送したことを確認できる。

【0060】なお、上記の説明において共通鍵暗号方法を利用して暗号化/復号を行なっているが、公開鍵暗号方法を利用しても当然構わない。また、Fiat Shamir 法をもとに説明したが、本方法は拡張Fiat Shamir 法(太田一岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告 ISEC88-13)を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコ

ルに 응용が可能である。

【0061】次に、本発明の第3実施例について説明する。

【0062】図7は本発明の第3の実施例における情報配送システムの構成を示すブロック図であり、10は情報提供者20から情報の提供を受ける利用者の端末（利用者端末）を示し、構成手段は図5に示す第2実施例と同様である。20は情報を提供する情報提供者の端末（情報提供者端末）を示し、200から206までの構成手段は第2実施例と同様であり、207は情報任意ビット長の複数のブロックに分割し、蓄積する情報分割手段、208は後日情報を利用者に配送した事実を証明する証拠としての通信履歴を記録管理する通信履歴ファイルである。30は第2実施例と同様に通信回線を表す。40は後日、情報提供者が通信履歴ファイル208に記録管理している通信履歴について、中立的立場によりその通信履歴の正当性を判定する調停者の端末（調停者端末）を表し、401は必要な演算を行う機能を有する演算手段、402は調停者が必要な情報を一時的に蓄積する一時メモリ、403は正当性の判定を依頼された通信履歴についてその正当性を検証する検証手段、404は情報を任意ビット長の複数のブロックに分割し、蓄積する情報分割手段である。

【0063】以下、図8のフローチャートにしたがって配送確認ステップでの動作手順を、また、図9のフローチャートにしたがって調停での動作手順を説明する。尚、準備段階は、前述した第2実施例と同様である。

【0064】（1）配送確認ステップ
情報提供者端末20は、利用者端末10に配送する情報Mを情報データベース202から取り出し（S121）、情報分割手段207において情報Mを任意ビット長サイズの複数のブロックに分割し、情報ブロック MB_j （ $j=1, 2, \dots, m$ ）として蓄積する（S122）。ここでは説明を簡単にするため、分割したブロック数を m 、全てのブロックについてビット長を g で一定とする。

【0065】これより以下の処理は第 j ブロックについてのものであり、第1ブロックから第 m ブロックまで各ブロックごとに以下の処理を順次（ m 回）繰り返し行う。

【0066】利用者端末10は、乱数発生手段103により g 個の乱数 R_{ij} （ $i=1, 2, \dots, g$ ）を生成した後一時メモリ102に蓄積し（S123）、それぞれの乱数について演算手段104により初期応答文 $X_{ij}=R_{ij}^2 \pmod{N1}$ （ $i=1, 2, \dots, g$ ）を計算した後一時メモリ102に蓄積する（S124）。その後、利用者秘密情報蓄積手段101に蓄積されているシステム秘密鍵 SK を秘密鍵として、共通鍵暗号手段105により暗号化した暗号化初期応答文 $CX_{ij}=E_{SK}(X_{ij})$ （ $i=1, 2, \dots, g$ ）を通信回線30を介して情報提

供者端末20に送信する（S125）。

【0067】情報提供者端末20は、受信した暗号化初期応答文 CX_{ij} （ $i=1, 2, \dots, g$ ）を情報提供者秘密情報蓄積手段201に蓄積されているシステム秘密鍵 SK を秘密鍵として、共通鍵暗号手段205により初期応答文 $X_{ij}=D_{SK}(CX_{ij})$ （ $i=1, 2, \dots, g$ ）に復号して、一時メモリ203に蓄積する（S126）。その後、情報提供者秘密情報蓄積手段201に蓄積されているシステム秘密鍵 SK を秘密鍵として、情報分割手段207に蓄積された情報ブロック MB_j を共通鍵暗号手段205により暗号化した暗号文ブロック $CB_j=E_{SK}(MB_j)$ を通信回線30を介して利用者端末10に送信する（S127）。

【0068】利用者端末10は、受信した暗号文ブロック CB_j を利用者秘密情報蓄積手段101に蓄積されているシステム秘密鍵 SK を秘密鍵として、共通鍵暗号手段105により情報ブロック $MB_j=D_{SK}(CB_j)$ に復号して、情報出力/利用手段106から情報ブロック MB_j を出力する（S128）。

【0069】さらに情報ブロック MB_j を出力すると同時に、演算手段104において情報ブロック MB_j と一時メモリ102に蓄積された初期応答文 X_{ij} （ $i=1, 2, \dots, g$ ）とを用いて一方向性ランダムハッシュ関数 h により検査文 $e_{ij}=h(MB_j \parallel X_{i1} \parallel X_{i2} \parallel \dots \parallel X_{ig})$ （ $i=1, 2, \dots, g$ ）を生成し（S129）、生成した検査文 e_{ij} のそれぞれのビット i に対し、一時メモリ102に蓄積された乱数 R_{ij} と利用者秘密情報蓄積手段101に蓄積された利用者の秘密情報 s とから $e_{ij}=0$ ならば $Y_{ij}=R_{ij}$ を、 $e_{ij}=1$ ならば $Y_{ij}=sR_{ij} \pmod{N1}$ を計算して（S130）、応答文 Y_{ij} （ $i=1, 2, \dots, g$ ）として情報提供者端末20に通信回線30を介して送信する（S131）。

【0070】情報提供者端末20は、受信した応答文 Y_{ij} （ $i=1, 2, \dots, g$ ）を一時メモリ203に蓄積し（S132）、その後、演算手段204において一時メモリ203に蓄積された初期応答文 X_{ij} （ $i=1, 2, \dots, g$ ）と情報分割手段207に蓄積された情報ブロック MB_j とを用いて、一方向性ランダムハッシュ関数 h により検査文 $e_{ij}=h(MB_j \parallel X_{i1} \parallel X_{i2} \parallel \dots \parallel X_{ig})$ （ $i=1, 2, \dots, g$ ）を生成し、一時メモリ203に蓄積する（S133）。

【0071】そして、検証手段206において利用者の公開情報 I および一時メモリ203に蓄積された初期応答文 X_{ij} と応答文 Y_{ij} と検査文 e_{ij} とからそれぞれのビット i に対し、 $e_{ij}=0$ ならば検証式 $Y_{ij}^2=X_{ij} \pmod{N1}$ を、 $e_{ij}=1$ ならば検証式 $Y_{ij}^2=X_{ij} \times I \pmod{N1}$ を満たすかどうかを検証する（S134）。この検証に失敗した場合には利用者は不正であると見做して直ちにプロトコルの実行を中止し（S135）、成功した場合には全てのブロックが終了するまで

以上の処理を繰り返す(S136)。そして、第1ブロックから第mブロックまでの全てのブロックについて検証に成功した場合には、一時メモリ203に蓄積された情報M、検査文 e_{ij} 、応答文 Y_{ij} ($i=1, 2, \dots, g: j=1, 2, \dots, m$)を通信履歴Hとして通信履歴ファイル208に記録管理する(S137)。

【0072】(2) 調停

後日、利用者が情報Mを受信していないと主張した場合には、情報提供者端末20は通信履歴ファイル208に記録管理された通信履歴Hを提示し、調停者端末40の一時メモリ402に蓄積する(S141)。

【0073】調停者端末40は、情報分割手段404において、一時メモリ402に蓄積された通信履歴中の情報Mについて、情報Mを複数の情報ブロック MB_j ($j=1, 2, \dots, m$)に分割して蓄積する(S142)。

【0074】各ブロック(第jブロック)について、演算手段401において利用者端末10の公開情報Iと一時メモリ402に蓄積された通信履歴H中の検査文 e_{ij} および応答文 Y_{ij} からそれぞれのビットiに対し、 $e_{ij}=0$ ならば $Y_{ij}=Y_{ij}^2 \pmod{N1}$ を、 $e_{ij}=1$ ならば $X_{ij}=Y_{ij}^2 / I \pmod{N1}$ を計算し、計算結果 X_{ij} ($i=1, 2, \dots, g$)を一時メモリ402に蓄積する(S143)。

【0075】次に、情報分割手段404に蓄積された情報ブロック MB_j と一時メモリ402に蓄積された計算結果 X_{ij} ($i=1, 2, \dots, g$)とから演算手段401の一方方向性ランダムハッシュ関数hにより検査文 $e_{ij}=h(MB_j \parallel X_{i1} \parallel X_{i2} \parallel \dots \parallel X_{ig})$ ($i=1, 2, \dots, g$)を生成する。(S144)。

【0076】その後、検証手段403において一時メモリ402に蓄積された通信履歴H中の検査文 e_{ij} ($i=1, 2, \dots, g$)と一致するかどうかを検査する(S145)。全てのブロック(第1ブロックから第mブロックまでのmブロック)について一致すれば(S146)、通信履歴Hの正当性が保証されたこととなり(S147)、そうでなければ通信履歴Hは無効となる(S148)。

【0077】上記の情報配送方法を用いて配送確認ステップが正常に終了したことは、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文 e_{ij} ($i=1, 2, \dots, g: j=1, 2, \dots, m$)が正しく生成されたことの証明となる。また、検査文 e_{ij} ($i=1, 2, \dots, g: j=1, 2, \dots, m$)は利用者が受信した情報ブロック MB_j ($j=1, 2, \dots, m$)と利用者が生成した初期応答文 X_{ij} ($i=1, 2, \dots, g: j=1, 2, \dots, m$)とから一方方向性ランダムハッシュ関数hを用いて生成されることから、正しい情報ブロック MB_j ($j=1, 2, \dots, m$)を受信しなければ正しい検査文 e_{ij} ($i=1, 2, \dots, g: j=1, 2, \dots, m$)を生成することはできない。したがって、検査

文 e_{ij} ($i=1, 2, \dots, g: j=1, 2, \dots, m$)を利用者が正しく生成できることと利用者が情報ブロック MB_j ($j=1, 2, \dots, m$)を正常に受信したことは同値となる。したがって、情報提供者は正確かつ確実に情報を利用者に配送したことを確認できる。

【0078】なお、上記の説明では、共通鍵暗号方法を利用して暗号化/復号を行った例を説明したが、公開鍵暗号方法を利用して当然構わない。また、Fiat Shamir法をもとに説明をしたが、本方法は拡張Fiat Shamir法(太田-岡本「Fiat-Shamir法の高次への拡張」、電子情報通信学会技術研究報告ISEC88-13)を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに対応が可能である。

【0079】次に、検査文 e_{ij} 、応答文 Y_{ij} 、($i=1, 2, \dots, g: j=1, 2, \dots, m$)、情報Mからなる通信履歴Hの関係では、ゼロ知識証明プロトコルにおける検証式と一方方向性ランダムハッシュ関数とにより相互に関係し合っているため、一部を不正に改竄するなどして通信履歴Hを偽造することは不可能である。したがって、通信履歴Hを記録管理することにより、情報Mを利用者が確実に受信していることの証拠として、後日、調停者などの中立的な第三者に提示することができる。

【0080】さらに、情報提供者端末と利用者端末との間の通信が情報Mの分割ブロック数mと同じ回数だけ繰り返し行われるため、途中で情報提供者の検証に失敗した場合にはそれ以降の通信は打ち切れ、残りの情報ブロックは送信されない。すなわち、利用者が知ることのできる情報ブロックは検証に失敗する以前のもののみに限られるので、情報提供者の検証を失敗させた利用者は結果として情報M全体を正しく受信することが不可能となる。したがって、利用者の秘密情報sを知らない不正な利用者が不正な応答文 Y_{ij} ($i=1, 2, \dots, g$)を送信する場合はもとより、応答文そのものを送信しないような不正行為を行い、情報提供者が情報Mを利用者に配送した事実を証明する通信履歴Hを情報提供者が記録管理できないにもかかわらず、利用者が情報M全体を不正に獲得してしまうことがないようにすることが可能である。

【0081】また、上記の説明では分割するブロックを各ブロックともビット長をgで一定としたが、例えば第1ブロックは1ビット、第2ブロックは2ビット、第3ブロックは4ビットというようにブロックごとにビット長サイズを変えても当然構わない。

【0082】以上の説明は、情報提供者が情報Mを正確かつ確実に利用者に配送したことを証明できるものであり、例えば著作物などの有料情報を情報Mとして配送する場合、あるいはあらかじめ暗号化されたソフトウェアなどをCD-ROM等により無償あるいは有償で配布した後、暗号化されたソフトウェアを復号するための鍵を

情報Mとして配送する場合、上記の情報配送方法によって情報提供者が利用者に情報Mを配送することにより、情報提供者が記録管理する通信履歴Hを著作権使用料等の情報料あるいはソフトウェアの販売代金を徴収するときの証明情報として利用できるなど、様々な利用が可能である。

【0083】次に、本発明の第4実施例について説明する。

【0084】図10は本発明の第4実施例における情報配送システムの構成を示すブロック図であり、10は情報提供者端末20から情報の提供を受ける利用者の端末（利用者端末）を示し、100から106までは第2実施例と同様の構成であり、107は公開鍵暗号方法（例えば、RSA, ElGamal）による暗号通信を行うための公開鍵暗号手段、108は分割されたブロック情報を元の情報再構成する情報再構成手段、109は情報提供者から受信した情報を蓄積する情報蓄積手段である。20は情報を提供する情報提供者の端末（情報提供者端末）を示し、200から208までは第3実施例と同様の構成であり、209は情報提供者が乱数を生成するための乱数発生手段、210は公開鍵暗号方法による暗号通信を行うための公開鍵暗号手段である。30は第2実施例と同様に通信回線である。40は調停者端末を表し、401から404までは第3実施例と同様の構成であり、405は公開鍵暗号方法による暗号化を行うための公開鍵暗号手段である。

【0085】以下、図11のフローチャートにしたがって配送確認ステップと情報取り出しステップでの動作手順を、また図12のフローチャートにしたがって調停での動作手順を説明する。

【0086】まず、準備段階として、信頼できるセンタが各利用者ごとに $p_1, q_1, I, s, p_2, q_2, P, U, S, U$ を設定し、このうち N_1, N_2, I, P, U を利用者の公開情報（公開鍵）として公開し、 s, S, U を利用者の秘密情報（秘密鍵）として利用者秘密情報蓄積手段101に蓄積して利用者に秘密裏に配布する。ここで、 (p_1, q_1) と (p_2, q_2) の各組はそれぞれ互いに異なる大きな素数の組になっており、 $N_1 = p_1 \times q_1, N_2 = p_2 \times q_2$ である。また、 $I = s^2 \pmod{N_1}, P \times S \equiv 1 \pmod{(p_2-1)(q_2-1)}$ が成立している。なお、 $p_1 = p_2, q_1 = q_2$ としてもよい。

【0087】(1) 配送確認ステップ

利用者端末10は、乱数発生手段103により $g \times m$ 個の乱数 R_{jk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$)を生成し、一時メモリ102に蓄積する(S151)。それぞれの乱数について演算手段104により初期応答文 $X_{jk} = R_{jk}^2 \pmod{N_1}$ ($j=1, 2, \dots, g; k=1, 2, \dots, m$)を計算し(S152)、通信回線30を介して情報提供者に送信する(S153)。

【0088】情報提供者端末20は、受信した初期応答文 X_{jk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$)を一時メモリ203に蓄積し(S154)、また乱数発生手段209により乱数文Zをランダムに生成して一時メモリ203に蓄積する(S155)。

【0089】次に、初期応答文 X_{jk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$)と乱数文Zとから演算手段204の一方方向性ランダムハッシュ関数hによりgビットサイズの情報暗号化用秘密鍵 $W_j = h(Z \parallel X_{11} \parallel X_{21} \parallel \dots \parallel X_{gm})$ ($j=1, 2, \dots, g$)を生成して一時メモリ203に蓄積する(S156)。ここで、一般にgの値は共通鍵暗号手段105および共通鍵暗号手段205で使用する秘密鍵の鍵長と等しいかそれ以上である。その後、配送する情報Mを情報データベース202から取り出し(S157)、情報暗号化用秘密鍵 W_j ($j=1, 2, \dots, g$)を秘密鍵として共通鍵暗号手段205により暗号文 $C = E, (M)$ に暗号化した後、利用者端末10に暗号文Cを通信回線30を介して送信する(S158)。

【0090】利用者端末10は、暗号文Cを情報蓄積手段109に受信/蓄積した後、受信した旨を通信回線30を介して情報提供者端末20に通知する(S159)。

【0091】情報提供者端末20は、一時メモリ203に蓄積された情報暗号化用秘密鍵 W_j ($j=1, 2, \dots, g$)を利用者の公開情報PUを用いて公開鍵暗号手段210により暗号化して検査文 $e_i = (W_1 \parallel W_2 \parallel \dots \parallel W_g)^{PU} \pmod{N_2}$ ($i=1, 2, \dots, L$)を生成する(S160)。なお、Lは N_2 のビット長に等しい。

【0092】次に、情報分割手段207において検査文 e_i ($i=1, 2, \dots, L$)を複数個のブロックに分割し、検査文ブロックとして蓄積する(S161)。ここでは説明を簡単にするため、分割したブロック数をm、全てのブロックについてビット長をgで一定とし、分割した検査文を検査文ブロック e_{Bjk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$)と表す。すなわち、 $e_{Bjk} = e_{(j+g(k-1))}$ であり、例えば $e_{B11} = e_1, e_{Bg1} = e_g, e_{B12} = e_{g+1}, e_{Bgm} = e_L$ のようになる。

【0093】これより以下の処理は第kブロックについてのものであり、第1ブロックから第mブロックまで各ブロックごとに以下の処理を順次(m回)繰り返す行う。

【0094】情報提供者端末20は、情報分割手段207に蓄積された検査文ブロック e_{Bjk} ($j=1, 2, \dots, g$)を通信回線30を介して利用者端末10に送信する(S162)。

【0095】利用者端末10は、受信した検査文ブロック e_{Bjk} ($j=1, 2, \dots, g$)を一時メモリ102に蓄積し(S163)、その後、演算手段104において

受信した検査文ブロック e_{jk} のそれぞれのビット j に対し、一時メモリ 102 に蓄積された乱数 R_{jk} と利用者秘密情報蓄積手段 101 に蓄積された利用者の秘密情報 s とから $e_{jk}=0$ ならば $Y_{jk}=R_{jk}$ を、 $e_{jk}=1$ ならば $Y_{jk}=s R_{jk} \pmod{N1}$ を計算して (S164)、応答文 Y_{jk} ($j=1, 2, \dots, g$) として情報提供者端末 20 に通信回線 30 を介して送信する (S165)。

【0096】情報提供者端末 20 は、受信した応答文 Y_{jk} ($j=1, 2, \dots, g$) を一時メモリ 203 に蓄積し (S166)、その後、検証手段 206 において利用者の公開情報 I および一時メモリ 203 に蓄積された初期応答文 X_{jk} と応答文 Y_{jk} と検査文 e_{jk} とからそれぞれのビット j に対し、 $e_{jk}=0$ ならば検証式 $Y_{jk}^2 = X_{jk} \pmod{N1}$ を、 $e_{jk}=1$ ならば検証式 $Y_{jk}^2 = X_{jk} \times I \pmod{N1}$ を満たすかどうかを検証する (S167)。この検証に失敗した場合には利用者は不正であると見做して直ちにプロトコルの実行を中止し (S168)、成功した場合には全てのブロックが終了するまで以上の処理を繰り返す (S169)。そして、第1ブロックから第 m ブロックまでの全てのブロックについて検証に成功した場合には、一時メモリ 203 に蓄積された乱数文 Z 、検査文 e_{jk} 、応答文 Y_{jk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$) を通信履歴 H として通信履歴ファイル 208 に記録管理する (S170)。

【0097】(2) 情報取り出しステップ

利用者端末 10 は、情報再構成手段 108 において、一時メモリ 102 に蓄積された検査文ブロック e_{jk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$) から検査文 e_i ($i=1, 2, \dots, L$) を再構成し (S171)、利用者秘密情報蓄積手段 101 に蓄積されている利用者の秘密情報 SU を用いて公開鍵暗号手段 107 により復号して情報暗号化用秘密鍵 $W_j = (e_1 \parallel e_2 \parallel \dots \parallel e_L)^{SU} \pmod{N2}$ ($j=1, 2, \dots, g$) を獲得した後、情報蓄積手段 109 に蓄積する (S172)。

【0098】最後に、情報蓄積手段 109 に蓄積された情報暗号化用秘密鍵 W_j ($j=1, 2, \dots, g$) を秘密鍵として、共通鍵暗号手段 105 により情報蓄積手段 109 に蓄積された暗号文 C を復号し、情報 $M=D$ 、 (C) を情報出力/利用手段 106 より獲得することができる (S173)。

【0099】(3) 調停

後日、利用者が情報 M を受信していないと主張した場合には、情報提供者端末 20 は通信履歴ファイル 208 に記録管理された通信履歴 H を提示し、調停者端末 40 の一時メモリ 402 に蓄積する (S181)。

【0100】調停者端末 40 は、各ブロック (第 k ブロック) について一時メモリ 402 に蓄積された通信履歴 H 中の検査文 e_{jk} および応答文 Y_{jk} からそれぞれのビット j に対し、演算手段 401 において $e_{jk}=0$ ならば $X_{jk}=Y_{jk}^2 \pmod{N1}$ を、 $e_{jk}=1$ ならば $X_{jk}=Y_{jk}^2 / I \pmod{N1}$ を計算し、計算結果 X_{jk} ($j=1, 2, \dots, g$) を一時メモリ 402 に蓄積する (S182)。

【0101】次いで、一時メモリ 402 に蓄積された計算結果 X_{jk} ($j=1, 2, \dots, g$) と乱数文 Z とを用いて演算手段 401 の一方向性ランダムハッシュ関数 h により g ビットサイズの情報暗号化用秘密鍵 $W_j = h(Z \parallel X_{11} \parallel X_{21} \parallel \dots \parallel X_{g1})$ ($j=1, 2, \dots, g$) を生成し (S183)、利用者の公開情報 P を用いて公開鍵暗号手段 405 により暗号化して検査文 $e_i = (W_1 \parallel W_2 \parallel \dots \parallel W_g)^P \pmod{N2}$ ($i=1, 2, \dots, L$) を生成する (S184)。

【0102】その後、情報分割手段 404 において検査文 e_i ($i=1, 2, \dots, L$) を複数個のブロックに分割して、検査文ブロック e_{jk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$) 生成し (S185)、最後に各ブロック (第 k ブロック) について、検証手段 403 において一時メモリ 402 に蓄積された通信履歴 H 中の検査文 e_{jk} ($j=1, 2, \dots, g$) と一致するかどうかを検査する (S186)。全てのブロック (第1ブロックから第 m ブロックまでの m ブロック) について一致すれば (S187)、通信履歴 H の正当性が証明されたことになり、利用者が情報 M を受信していることが保証されたこととなり (S188)、そうでなければ通信履歴 H は無効とされる (S189)。

【0103】上記の情報配送方法を用いれば、情報 M 本体は初めに暗号文 C に暗号化されて利用者に送信されるため、暗号文 C を利用者が受信した時点では情報 M を獲得されることはない。そして、ゼロ知識証明プロトコルが正常に終了した時点で、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文 e_{jk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$) を利用者が正しく受信したことの証明となる。

【0104】また、検査文 e_{jk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$) を利用者が復号することにより情報暗号化用秘密鍵 W_j ($j=1, 2, \dots, g$) を生成し、生成した情報暗号化用秘密鍵 W_j ($j=1, 2, \dots, g$) を用いて暗号文 C を復号して情報 M を獲得することができる。したがって、検査文 e_{jk} ($j=1, 2, \dots, g; k=1, 2, \dots, m$) を利用者が正しく受信したことから利用者が情報 M を正常に受信したことは同値となる。したがって、情報提供者は正確かつ確実に情報を利用者に配送したことを確認できる。

【0105】なお、上記の説明において公開鍵暗号方法を利用して暗号化/復号を行っているが、共通鍵暗号方法を利用しても当然構わない。また、Fiat Shamir 法をもとに説明したが、本方法は拡張 Fiat Shamir 法 (太田一岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告 ISEC88-13) を始めとす

る、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに 응용が可能である。

【0106】次に、検査文 e_{jk} 、応答文 Y_{jk} 、($j = 1, 2, \dots, g; k = 1, 2, \dots, m$)、乱数文 Z からなる通信履歴 H の関係では、ゼロ知識証明プロトコルにおける検証式と一方方向性ランダムハッシュ関数とにより相互に関係し合っているため、一部を不正に改竄するなどして通信履歴 H を偽造することは不可能である。したがって、通信履歴 H を記録管理することにより、情報暗号化用秘密鍵 W_j ($j = 1, 2, \dots, g$)を利用者が確実に受信していることの証拠として、後日、調停者などの中立的な第三者に提示することができる。

【0107】さらに、情報提供者と利用者との間の通信が情報暗号化用秘密鍵 W_j ($j = 1, 2, \dots, g$)の分割ブロック数 m と同じ回数だけ繰り返されるため、途中で情報提供者の検証に失敗した場合にはそれ以降の通信は打ち切れ、残りの検査文は送信されない。すなわち、利用者が知ることのできる検査文は検証に失敗する以前のもののみに限られるので、情報提供者の検証を失敗させた利用者は暗号文 C を復号するために必要な情報の一部しか獲得することができず、結果として正しい情報暗号化用秘密鍵 W_j ($j = 1, 2, \dots, g$)を生成することが不可能となる。したがって、利用者の秘密情報 s を知らない不正な利用者が不正な応答文 Y_{jk} ($j = 1, 2, \dots, g; k = 1, 2, \dots, m$)を送信する場合はもとより、応答文そのものを送信しないような不正行為を行い、情報提供者が情報 M を利用者に配送した事実を証明する通信履歴 H を情報提供者が記録管理できないにもかかわらず、利用者が情報 M を獲得するのに必要な検査文 e_{jk} ($j = 1, 2, \dots, g; k = 1, 2, \dots, m$)を受信し、情報 M を不正に復号/獲得してしまうことがないようにすることが可能である。また、上記の説明では分割するブロックを各ブロックともビット長を g で一定としたが、例えば第1ブロックは1ビット、第2ブロックは2ビット、第3ブロックは4ビットというようにブロックごとにビット長サイズを変えても当然構わない。

【0108】以上の説明は、情報提供者が大容量の情報 M を正確かつ確実に利用者に配送したことを証明できるものであり、例えば情報 M を著作物などの「オンデマンドサービス」としての有料情報とした場合、上記の情報配送方法によって情報提供者が利用者に情報 M を配送することにより、情報提供者が記録管理する通信履歴 H を著作権使用料等の情報料を徴収するときの証明情報として利用できるなど、様々な利用が可能である。

【0109】以上説明したとおり、本発明の第2～第4実施例のゼロ知識証明プロトコルを利用した情報配送方法では、第一にプロトコルの動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知

識証明プロトコルと同様に、不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第二に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了した事実と同値であるので、情報提供者は正しい利用者が情報を正しく受信していると判断できる。

【0110】又、情報を暗号化し暗号文として送信することにより、第三者による情報の盗聴を防止し、かつ第三者が情報を解読するために有効な情報も得られないようにすることもできる。

【0111】又、本発明の第2実施例によれば、暗号文の復号処理を配送確認ステップと切り離して実行することができる。

【0112】又、本発明の第2、第3実施例によれば、例えばハッシュ関数などを用いて情報（または利用者が復号可能な暗号文）から検査文を生成することにより検査文のサイズを小さくすることができ、配送確認ステップにおける通信量及び処理時間を削減できる。

【0113】又、本発明の第3実施例によれば、一方方向性関数を用いて検査文を生成することにより、情報（または利用者が復号可能な暗号文）、応答文、及び検査文とからなる通信履歴の偽造を不可能にする。

【0114】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者のプロトコルに失敗した場合には、直ちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者に送信されないことになるため、結果として情報（または利用者が復号可能な暗号文）全てを不正に獲得してしまうことがないようにできる。

【0115】又、本発明の第4実施例によれば、大容量の情報を送信する場合に、第一に情報は情報提供者が生成した情報暗号化用秘密鍵によって初めに暗号化されて利用者に配送されるため、利用者の認証が行われる以前に情報本体を利用者が取り出すことはできない。第二に情報暗号化用秘密鍵についてのみ検査文として配送確認を行うことにより、通信量及び配送確認のための処理時間を大幅に短縮できる。第三に配送確認ステップが正常に終了すれば利用者は検査文を正しく受信したことが確認でき、情報取り出しステップにおいて情報暗号化用秘密鍵を獲得することが保証されるので、この時点で初めて情報を間違いなく取り出すことができる。したがって、これらの効果により情報配送方法が終了した場合には、情報提供者は正規の利用者に対して情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は情報を利用者まで確実に配送したと判断できる。

【0116】又、一方方向性関数を用いて情報暗号化用秘密鍵を生成することにより情報提供者にとって都合の良い情報暗号化用秘密鍵を不正に生成できないようにする

ことができる。また、同様に方向性関数を用いることにより、乱数文と検査文と応答文とからなる通信履歴を偽造することは不可能になるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【0117】又、検査文について暗号通信を行うことは、情報暗号化用秘密鍵についても暗号通信を行なっていることと同等の効果が得られるため、第三者による情報暗号化用秘密鍵の盗聴を防止し、かつ第三者が情報暗号化用秘密鍵を解読するために有効な情報も得られないようになる。

【0118】又、検査文の復号処理を配送確認ステップと切り離して実行することができる。

【0119】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者には送信されないことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として情報本体もしくは情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【0120】又、本発明の第3、第4実施例によれば、偽造不可能な通信履歴を実際に情報を配送した証拠として記録管理することができ、かつ必要に応じて提示できるようになる。さらに、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平5-12321）の方式と比較して大幅に削減できる。

【0121】又、情報提供者と利用者間で情報の提供の有無について調停を行う必要が生じた場合、情報提供者が通信履歴を裁判所等の中立な調停機関に提示し、調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。すなわち、情報提供者が利用者に対して情報（または利用者が復号可能な暗号文）を送信し、かつ利用者が確実に受信したことを、後日調停者が確認できるので、利用者が情報（または利用者が復号可能な暗号文）を受信しているにも関わらず、利用者が情報を受信していないなどという不当な主張を防止できる。

【0122】又、これらの実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【0123】又、情報提供者と利用者間で暗号通信ができるようにしたシステムとなる。

【0124】又、本発明の第4実施例によれば、情報提供者から提供された情報を蓄積し、利用者が必要に応じて情報を利用できるようにしたシステムとなる。

【0125】又、情報暗号化用秘密鍵の生成機能を有し、情報暗号化用秘密鍵を用いた情報配送ができるようにしたシステムとなる。

【0126】又、本発明の第3、第4実施例によれば、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【0127】又、不正な利用者であることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【0128】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【0129】次に本発明の第5実施例について説明する。

【0130】図13は本発明の第5実施例における情報配送システムの構成を示すブロック図であり、10は情報提供者に対して情報の配送を必要とする利用者（端末）を示し、100は通信回線30を制御する通信制御手段、101はセンタが作成し利用者の秘密情報を蓄積しておく利用者秘密情報蓄積手段、105は共通鍵暗号方法（例えば、DES、FEAL）による暗号通信を行うための共通鍵暗号手段、107は公開鍵暗号方法（例えば、RSA）による暗号通信を行うための公開鍵暗号手段、109は情報提供者から配送された情報を蓄積する情報蓄積手段、102は利用者が必要な情報を一時的に蓄積する一時メモリ、103は利用者が乱数を生成するための乱数発生手段、104は必要な演算を行う演算手段、106は利用者が要求した情報を出力もしくは利用する情報出力/利用手段である。

【0131】また、20は情報を提供する情報提供者（端末）を示し、200は通信回線30を制御する通信制御手段、201はセンタが作成した情報提供者の秘密情報を蓄積しておく情報提供者秘密情報蓄積手段、205は共通鍵暗号方法による暗号通信を行うための共通鍵暗号手段、210は公開鍵暗号方法による暗号通信を行うための公開鍵暗号手段、202は提供する情報が蓄積してある情報データベース、203は情報提供者が必要な情報を一時的に蓄積する一時メモリ、209は情報提供者が乱数を生成するための乱数発生手段、204は必要な演算を行う演算手段、206はFiat Shamir 法に基づいて通信系列の正当性を検証する検証手段である。30は利用者と情報提供者とを通信で接続する通信回線を表す。

【0132】以下、図14のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を説明する。

【0133】まず基準段階として、信頼できるセンタが各利用者ごとに $p_1, q_1, I, s, p_2, q_2, P, U, S, U$ を設定し、このうち N_1, N_2, I, P, U を利用者の公開情報（公開鍵）として公開し、 s, S, U を利用者の秘密情報（秘密鍵）として利用者秘密情報蓄積手段101に蓄積して利用者に秘密裏に配布する。ここで、 (p_1, q_1) と (p_2, q_2) の各組はそれぞれ互いに異なる大きな素数の組になっており、 $N_1 = p_1 \times q_1, N_2 = p_2 \times q_2$ である。また、 $I = s^2 \pmod{N_1}, P \times U = 1 \pmod{(p_2-1)(q_2-1)}$ が成立している。なお、 $p_1 = p_2, q_1 = q_2$ としてもよい。

【0134】さらに、各情報提供者ごとに p, q, P, C, S, C を設定し、このうち N, P, C を情報提供者の公開情報（公開鍵）として公開し、 S, C を情報提供者の秘密情報（秘密鍵）として情報提供者秘密情報蓄積手段201に蓄積して情報提供者に秘密裏に配布する。ここで、 p, q は互いに異なる大きな素数であり、 $N = p \times q$ である。また、 $P \times C = 1 \pmod{(p-1)(q-1)}$ が成立している。

【0135】(1) 情報配送ステップ

情報提供者は、乱数発生手段209により g ビットサイズの情報暗号化用秘密鍵 W_i ($i = 1, 2, \dots, g$)を生成して一時メモリ203に蓄積する(S201)。ここで、一般に g の値は共通鍵暗号手段105, 205で使用する秘密鍵の鍵長と等しいかそれ以上ある。なお、ここでは情報暗号化用秘密鍵 W_i ($i = 1, 2, \dots, g$)について乱数発生手段209により生成しているが、実際には関数を使用して生成したり、あるいは特定の秘密鍵を一意的に使用するなどしても構わない。

【0136】次に、利用者に配送する情報 M を情報データベース202から取り出し(S202)、情報暗号化用秘密鍵 W_i ($i = 1, 2, \dots, g$)を秘密鍵として共通鍵暗号手段205により暗号文 $C = E_i(M)$ に暗号化した後(S203)、利用者に暗号文 C を通信回線30（および通信制御手段100, 200）を介して送信する(S204)。

【0137】利用者は、暗号文 C を情報蓄積手段109に受信／蓄積した後、受信した旨を通信回線30を介して情報提供者に通知する(S205)。

【0138】(2) 配送確認ステップ

利用者は、乱数発生手段103により g 個の乱数 R_i ($i = 1, 2, \dots, g$)を生成し、一時メモリ102に蓄積した後(S206)、それぞれの乱数について演算手段104により初期応答文 $X_i = R_i^2 \pmod{N_1}$ ($i = 1, 2, \dots, g$)を計算し(S207)、情報提供者の公開鍵 P, C を用いて公開鍵暗号手段107に

より暗号化初期応答文 $CX_i = X_i^P \pmod{N}$ ($i = 1, 2, \dots, g$)に暗号化して(S208)、通信回線30を介して情報提供者に送信する(S209)。

【0139】情報提供者は、情報提供者秘密情報蓄積手段201に蓄積された秘密鍵 S, C を用いて公開鍵暗号手段210により受信した暗号化初期応答文 CX_i を初期応答文 $X_i = CX_i^S \pmod{N}$ ($i = 1, 2, \dots, g$)に復号した後、一時メモリ203に蓄積する(S210)。

【0140】次に、一時メモリ203に蓄積された情報暗号化用秘密鍵 W_i ($i = 1, 2, \dots, g$)を秘密鍵配送文 V_i および検査文 e_i ($i = 1, 2, \dots, g$)として一時メモリ203に蓄積した後(S211)、利用者の公開鍵 P, U を用いて公開鍵暗号手段210により暗号化検査文 $Ce_i = (e_i \parallel e_2 \parallel \dots \parallel e_g)^U \pmod{N_2}$ ($i = 1, 2, \dots, |N_2|$)に暗号化して(S212)、通信回線30を介して送信する(S213)。ここで、 $|N_2|$ は N_2 のビット数を表す。

【0141】利用者は、利用者秘密情報蓄積手段101に蓄積された秘密鍵 S, U を用いて公開鍵暗号手段107により受信した暗号化検査文 Ce_i ($i = 1, 2, \dots, g$)を検査文 $e_i = (Ce_i \parallel Ce_2 \parallel \dots \parallel Ce_{|N_2|})^U \pmod{N_2}$ ($i = 1, 2, \dots, g$)に復号した後、一時メモリ102に蓄積する(S214)。

【0142】次に、演算手段104において検査文 e_i のそれぞれのビット i に対し、一時メモリ102に蓄積された乱数 R_i と利用者秘密情報蓄積手段101に蓄積された利用者の秘密情報 s とから $e_i = 0$ ならば $Y_i = R_i$ を、 $e_i = 1$ ならば $Y_i = s R_i \pmod{N_1}$ を計算し(S215)、応答文 Y_i ($i = 1, 2, \dots, g$)として情報提供者に通信回線30を介して送信する(S216)。

【0143】情報提供者は、受信した応答文 Y_i ($i = 1, 2, \dots, g$)を一時メモリ203に蓄積した(S217)後、検証手段206において利用者の公開情報 I および一時メモリ203に蓄積された初期応答文 X_i と応答文 Y_i と検査文 e_i とからそれぞれのビット i に対し、 $e_i = 0$ ならば検証式 $Y_i^2 = X_i \pmod{N_1}$ を、 $e_i = 1$ ならば検証式 $Y_i^2 = X_i \times I \pmod{N_1}$ を満たすかどうかを検証する(S218)。この検証に失敗した場合には利用者は不正であるとみなしてそれ以降の利用を禁止し(S219A)、そうでなければ正常に終了する(S219B)。

【0144】(3) 情報取り出しステップ

利用者は、一時メモリ102に蓄積された検査文 e_i ($i = 1, 2, \dots, g$)から演算手段104において秘密鍵配送文 V_i および情報暗号化用秘密鍵 W_i ($i = 1, 2, \dots, g$)を取り出し、情報蓄積手段109に蓄積する(S220)。

【0145】最後に、情報蓄積手段109に蓄積された

情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を秘密鍵として、共通鍵暗号手段105により情報蓄積手段109に蓄積された暗号文 C を復号し(S221)、要求した情報 $M=D_i(C)$ を情報出力/利用手段106より獲得することができる(S222)。

【0146】上記の情報配送方法を用いれば、情報 M は初めに暗号文 C に暗号化されて利用者に送信されるため、暗号文 C を利用者が受信した時点では情報 M を獲得されることはない。そして、ゼロ知識証明プロトコルが正常に終了した時点で、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文 e_i ($i=1, 2, \dots, g$)を利用者が正常に受信し、適切な処理を行っていることがわかる。

【0147】また、利用者は検査文 e_i ($i=1, 2, \dots, g$)を正しく受信していれば情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を生成し、利用者が要求した情報の暗号文 C を復号して情報 M を獲得することができるため、検査文 e_i ($i=1, 2, \dots, g$)を利用者が正常に受信したことと利用者が要求した情報を正常に受信したことは同値となる。したがって、情報提供者は要求された情報を正確かつ確実に利用者に配送したことを確認できる。

【0148】なお、上記の説明において公開鍵暗号方法を利用して暗号化/復号を行っている部分については、共通鍵暗号方法を利用しても当然構わない。また、上記の説明ではFiat Shamir法をもとに説明したが、本方法は拡張Fiat Shamir法(太田-岡本「Fiat-Shamir法の高次への拡張」、電子情報通信学会技術研究報告ISEC88-13)を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【0149】次に、本発明の第6実施例について説明する。

【0150】図15は本発明の第6の実施例における情報配送システムの構成を示すブロック図であり、システム構成は情報提供者(端末)20の情報提供者秘密情報蓄積手段201が必要ないことを除き、第5実施例の構成と同様である。

【0151】以下、図16のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を説明する。

【0152】まず、準備段階として、信頼できるセンタが各利用者ごとに $p_1, q_1, I, s, p_2, q_2, P, U, SU$ を設定し、このうち N_1, N_2, I, P, U を利用者の公開情報(公開鍵)として公開し、 s, SU を利用者の秘密情報(秘密鍵)として利用者秘密情報蓄積手段101に蓄積して利用者に秘密裏に配布する。ここで、 (p_1, q_1) と (p_2, q_2) の各組はそれぞれ互いに異なる大きな素数の組になっており、 $N_1=p_1 \times q_1, N_2=p_2 \times q_2$ である。また、 $I=s^2 \pmod{N_1}$ 、 $PU \times SU=1 \pmod{(p_2-1)(q_2-1)}$ が成立している。なお、 $p_1=p_2, q_1=q_2$ としてもよい。

【0153】(1) 情報配送ステップ
第5実施例と同様である(S231~235)。

(2) 配送確認ステップ
利用者は、乱数発生手段103により $|N_2|$ 個の乱数 R_i ($i=1, 2, \dots, |N_2|$)を生成し、一時メモリ102に蓄積した後(S236)、それぞれの乱数について演算手段104により初期応答文 $X_i=R_i^2 \pmod{N_1}$ ($i=1, 2, \dots, |N_2|$)を計算し(S237)、通信回線30を介して情報提供者に送信する。(S238)。ここで、 $|N_2|$ は N_2 のビット数を表す。

【0154】情報提供者は、受信した初期応答文 X_i ($i=1, 2, \dots, |N_2|$)を一時メモリ203に蓄積する(S239)。次に、一時メモリ203に蓄積された情報暗号化用秘密鍵 W_i を秘密鍵配送文 V_i ($i=1, 2, \dots, g$)として利用者の公開鍵 P, U を用いて公開鍵暗号手段210により暗号化し、検査文 $e_i=(V_1 \parallel V_2 \parallel \dots \parallel V_g)^{PU} \pmod{N_2}$ ($i=1, 2, \dots, |N_2|$)を生成した後、一時メモリ203に蓄積する(S240)。その後、検査文 e_i ($i=1, 2, \dots, |N_2|$)を通信回線30を介して送信する(S241)。

【0155】利用者は、受信した検査文 e_i ($i=1, 2, \dots, |N_2|$)を一時メモリ102に蓄積した後(S242)、演算手段104において検査文 e_i のそれぞれのビット i に対し、一時メモリ102に蓄積された乱数 R_i と利用者秘密情報蓄積手段101に蓄積された利用者秘密情報 s とから $e_i=0$ ならば $Y_i=R_i$ を、 $e_i=1$ ならば $Y_i=s R_i \pmod{N_1}$ を計算し(S243)、応答文 Y_i ($i=1, 2, \dots, g$)として情報提供者に通信回線30を介して送信する(S244)。

【0156】情報提供者は、受信した応答文 Y_i ($i=1, 2, \dots, |N_2|$)を一時メモリ203に蓄積した後(S245)、検証手段206において利用者の公開情報 I および一時メモリ203に蓄積された初期応答文 X_i と応答文 Y_i と検査文 e_i とからそれぞれのビット i に対し、 $e_i=0$ ならば検証式 $Y_i^2=X_i \pmod{N_1}$ を、 $e_i=1$ ならば検証式 $Y_i^2=X_i \times I \pmod{N_1}$ を満たすかどうかを検証する(S246)。この検証に失敗した場合には利用者は不正であるとみなしてそれ以降の利用を禁止し(S247A)、そうでなければ正常に終了する(S247B)。

【0157】(3) 情報取り出しステップ
利用者は、一時メモリ102に蓄積された検査文 e_i ($i=1, 2, \dots, |N_2|$)を利用者秘密情報蓄積手段101に蓄積された秘密鍵 SU を用いて公開鍵暗号

手段107により秘密鍵配送文 $V_i = (e_1 \parallel e_2 \parallel \dots \parallel e_{1/2})^{SU} \pmod{N2}$ ($i=1, 2, \dots, g$)に復号した(S248)後、演算手段104において情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を取り出し、情報蓄積手段109に蓄積する(S249)。

【0158】最後に、情報蓄積手段109に蓄積された情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を秘密鍵として、共通鍵暗号手段105により情報蓄積手段109に蓄積された暗号文Cを復号し(S250)、要求した情報 $M=D_c(C)$ を情報出力/利用手段106より獲得することができる(S251)。

【0159】上記の情報配送方法を用いれば、第5実施例と全く同等の効果が得られる。また第5実施例と比較して、一時メモリ等に蓄積しなければならない情報量のサイズは大きくなるが、処理速度の遅い公開鍵暗号方法を利用する回数が1回ですむため、処理時間の短縮化が期待できる。

【0160】なお、上記の説明において公開鍵暗号方法を利用して暗号化/復号を行っている部分については共通鍵暗号方法を利用しても当然構わない。また、上記の説明ではFiat Shamir法をもとに説明したが、本方法は拡張Fiat Shamir法(太田-岡本「Fiat-Shamir法の高次への拡張」、電子情報通信学会技術研究報告ISEC88-13)を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【0161】次に、本発明の第7実施例について説明する。

【0162】図17は本発明の第7の実施例における情報配送システムの構成を示すブロック図であり、10は利用者(端末)を示し、公開鍵暗号手段107が必要ないことを除いて100から109までの構成手段は第6実施例と同様であり、110は情報配送要求文を作成する入力手段である。20は情報提供者(端末)を示し、公開鍵暗号手段210が必要ないことを除いて200から206までと209の構成手段は第6実施例と同様であり、208は後日、情報を利用者に配送した事実を証明する証拠としての通信履歴Hを記録管理する通信履歴ファイルである。30は利用者と情報提供者とを通信で接続する通信回線を表す。40は後日、情報提供者が通信履歴ファイル208に記録管理している通信履歴Hについて、中立的立場によりその通信履歴Hの正当性を判定する調停者(端末)を表し、402は調停者が必要な情報を一時的に蓄積する一時メモリ、401は必要な演算を行う演算手段、403は正当性の判定を依頼された通信履歴Hについてその正当性を検証する検証手段である。

【0163】以下、図18のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を、また図19のフローチャートに

したがって調停での動作手順を説明する。

【0164】まず、準備段階として、信頼できるセンタが各利用者ごとに $p1, q1, I, s$ を設定し、このうち $N1$ と I を利用者の公開情報として公開し、 s を利用者の秘密情報として利用者秘密情報蓄積手段101に蓄積して利用者に秘密裏に配布する。ここで、 $p1$ と $q1$ は互いに異なる大きな素数を表し、 $N1=p1 \times q1$ である。また、 $I=s^2 \pmod{N1}$ が成立している。

【0165】(1) 情報配送ステップ

利用者は、情報提供者に提供して欲しい情報について入力手段110から情報配送要求文RSを作成し、一時メモリ102に蓄積した(S261)後、通信回線30を介して情報提供者に送信する(S262)。ここで、情報配送要求文RSは、例えば図20に示すように要求日時、利用者識別番号、要求情報名、要求情報コード等から構成される。なお、図20は情報配送要求文RSの構成形態を表している。

【0166】ここでは情報配送要求文RSを利用者より情報提供者に送信しているが、実際には要求情報コードのみを利用者が情報提供者に送信するなどして、情報提供者と利用者がそれぞれ独自に同じ情報配送要求文RSを作成するようにしてもよい。

【0167】情報提供者は、乱数発生手段209により乱数文Zをランダムに生成し(S263)、情報配送要求文RSと生成した乱数文Zとを一時メモリ203に蓄積した(S264)後、情報配送要求文RSと乱数文Zとから演算手段204中の第一の方向性ランダムハッシュ関数 $f1$ により g ビットサイズの情報暗号化用秘密鍵 $W_i = f1(RS, Z)$ ($i=1, 2, \dots, g$)を生成して一時メモリ203に蓄積する(S265)。ここで、一般に g の値は共通鍵暗号手段105、205で使用する秘密鍵の鍵長と等しいかそれ以上である。次に、情報配送要求文RS中の要求情報コードをもとに、そのコードに対応する情報Mを情報データベース202から取り出し(S266)、情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を秘密鍵として共通鍵暗号手段205により暗号文 $C=E_{W_i}(M)$ に暗号化した(S267)後、利用者に暗号文Cを通信回線30を介して送信する(S268)。

【0168】利用者は、暗号文Cを情報蓄積手段109に受信/蓄積した後、受信した旨を通信回線30を介して情報提供者に通知する(S269)。

【0169】(2) 配送確認ステップ

利用者は、乱数発生手段103により g 個の乱数 r_i ($i=1, 2, \dots, g$)を生成した後一時メモリ102に蓄積し(S270)、それぞれの乱数について演算手段104により初期応答文 $X_i = R_i^2 \pmod{N1}$ ($i=1, 2, \dots, g$)を計算した後一時メモリ102に蓄積し(S271)、初期応答文 X_i ($i=1, 2, \dots, g$)を通信回線30を介して情報提供者に送信する

(S272)。

【0170】情報提供者は、受信した初期応答文 X_i ($i=1, 2, \dots, g$)を一時メモリ203に蓄積した(S273)後、一時メモリ203に蓄積された情報配送要求文RSと初期応答文 X_i ($i=1, 2, \dots, g$)とから演算手段204中の第二の方向性ランダムハッシュ関数 f_2 により g ビットサイズの鍵暗号化用秘密鍵 $K_i = f_2(RS, (X_1 \parallel X_2 \parallel \dots \parallel X_g))$ ($i=1, 2, \dots, g$)を生成し、一時メモリ203に蓄積する(S274)。なお、 f_1 と f_2 は同じ関数で

ここで、第三の関数 f_3 には例えば $V_i = f_3(W_i, K_i) - W_i \oplus K_i$ ($i=$

$1, 2, \dots, g$)がある。なお、 \oplus は排他的論理和を表す。

利用者は、受信した検査文 e_i ($i=1, 2, \dots, g$)を一時メモリ102に蓄積した(S277)後、演算手段104において検査文 e_i のそれぞれのビット i に対し、一時メモリ102に蓄積された乱数 R_i と利用者秘密情報蓄積手段101に蓄積された利用者の秘密情報 s とから $e_i=0$ ならば $Y_i = R_i$ を、 $e_i=1$ ならば $Y_i = s R_i \pmod{N1}$ を計算し(S278)、応答文 Y_i ($i=1, 2, \dots, g$)として情報提供者に通信回線30を介して送信する(S279)。

【0172】情報提供者は、受信した応答文 Y_i ($i=1, 2, \dots, g$)を一時メモリ203に蓄積した(S280)後、検証手段206において利用者の公開情報 I および一時メモリ203に蓄積された初期応答文 X_i と応答文 Y_i と検査文 e_i とからそれぞれのビット i に対し、 $e_i=0$ ならば検証式 $Y_i^2 = X_i \pmod{N1}$ を、 $e_i=1$ ならば検証式 $Y_i^2 = X_i \times I \pmod{N1}$ を満たすかどうかを検証する(S281)。この検証に失敗した場合には利用者は不正であるとみなしてそれ以降の利用を禁止し(S282)、成功した場合には図21に示すように、一時メモリ203に蓄積された情

5)。ここで、例えば第三の関数 f_3 の $V_i = f_3(W_i, K_i) - W_i \oplus K_i$

($i=1, 2, \dots, g$)に対し、第三の逆関数 f_3' は $W_i = f_3'(V_i, K_i) - V_i \oplus K_i$ ($i=1, 2, \dots, g$)となる。なお、 \oplus は排他的論理和を表

す。

【0174】最後に、情報蓄積手段109に蓄積された情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を秘密鍵として共通鍵暗号手段105により情報蓄積手段109に蓄積された暗号文 C を復号し(S286)、要求した情報 $M = D_v(C)$ を情報出力/利用手段106より獲得することができる(S287)。

【0175】(4) 調停

後日、利用者が要求した情報を受信していないと主張したり、情報配送の要求そのものを否定した場合には、情報提供者は通信履歴ファイル208に記録管理された通

も当然構わない。

【0171】次に、一時メモリ203に蓄積された情報暗号化用秘密鍵 W_i と鍵暗号化用秘密鍵 K_i ($i=1, 2, \dots, g$)とから演算手段204中の第三の関数 f_3 により秘密鍵配送文 V_i ($i=1, 2, \dots, g$)を生成し、検査文 e_i ($i=1, 2, \dots, g$)として一時メモリ203に蓄積した(S275)後、利用者に検査文 e_i ($i=1, 2, \dots, g$)を通信回線30を介して送信する(S276)。こ

【外1】

報配送要求文RS、乱数文Z、検査文 e_i 、応答文 Y_i ($i=1, 2, \dots, g$)を通信履歴Hとして通信履歴ファイル208に記録管理する(S283)。なお、図21は通信履歴Hの構成形態を示している。

【0173】(3) 情報取り出しステップ

利用者は、一時メモリ102に蓄積された情報配送要求文RSと初期応答文 X_i ($i=1, 2, \dots, g$)とから演算手段104中の第二の方向性ランダムハッシュ関数 f_2 により g ビットサイズの鍵暗号化用秘密鍵 $K_i = f_2(RS, (X_1 \parallel X_2 \parallel \dots \parallel X_g))$ ($i=1, 2, \dots, g$)を生成し、一時メモリ102に蓄積する(S284)。次に、一時メモリ102に蓄積された検査文 e_i ($i=1, 2, \dots, g$)から秘密鍵配送文 V_i ($i=1, 2, \dots, g$)を生成し、生成した秘密鍵配送文 V_i と鍵暗号化用秘密鍵 K_i ($i=1, 2, \dots, g$)とから演算手段104中の第三の関数 f_3 の逆関数 f_3' により情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を取り出し、情報蓄積手段109に蓄積する(S288)

【外2】

信履歴Hを提示し、調停者の一時メモリ402に蓄積する(S291)。

【0176】調停者は、演算手段401において利用者の公開情報 I と一時メモリ402に蓄積された通信履歴H中の検査文 e_i および応答文 Y_i からそれぞれのビット i に対し、 $e_i=0$ ならば、 $X_i = Y_i^2 \pmod{N1}$ を $e_i=1$ ならば $X_i = Y_i^2 / I \pmod{N1}$ を計算し、一時メモリ402に蓄積する(S292)。

【0177】次に、一時メモリ402に蓄積された通信履歴H中の配送要求文RSと乱数文Zとから演算手段401中の第一の方向性ランダムハッシュ関数 f_1 によ

り情報暗号化用秘密鍵 $W_i = f_1(RS, Z)$ ($i = 1, 2, \dots, g$) を (S293)、また情報配送要求文 RS と計算結果 X_i ($i = 1, 2, \dots, g$) とから演算手段401中の第二の一方方向性ランダムハッシュ関数 f_2 により鍵暗号化用秘密鍵 $K_i = f_2(RS, (X_i \parallel X_2 \parallel \dots \parallel X_g))$ ($i = 1, 2, \dots, g$) をそれぞれ生成し、一時メモリ402に蓄積する (S294)。そして、情報暗号化用秘密鍵 W_i と鍵暗号化用秘密鍵 K_i ($i = 1, 2, \dots, g$) とから演算手段401中の第三の関数 f_3 により秘密鍵配送文 V_i ($i = 1, 2, \dots, g$) を生成し (S295)、検査文 e_i ($i = 1, 2, \dots, g$) として検証手段403において一時メモリ402に蓄積された通信履歴 H 中の検査文 e_i ($i = 1, 2, \dots, g$) と一致するかどうかを検査する (S296)。一致すれば、通信履歴 H の正当性が証明されたことになり (S297)、利用者が情報配送を要求し、かつ要求した情報を受信していることが保証される。そうでなければ通信履歴 H は無効とされる (S298)。

【0178】上記の情報配送方式を用いれば、情報 M は初めに暗号文 C に暗号化されて利用者に送信されるため、暗号文 C を利用者が受信した時点では情報 M を獲得されることはない。そして、ゼロ知識証明プロトコルが正常に終了した時点で、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文 e_i ($i = 1, 2, \dots, g$) を利用者が正常に受信したことの証明となる。

【0179】また、検査文 e_i ($i = 1, 2, \dots, g$) の他は利用者自身が作成した情報配送要求文 RS と初期応答文 X_i ($i = 1, 2, \dots, g$) とから情報暗号化用秘密鍵 W_i ($i = 1, 2, \dots, g$) を生成し、利用者が暗号文 C を復号して要求した情報 M を獲得することができるため、検査文 e_i ($i = 1, 2, \dots, g$) を利用者が正常に受信したことと利用者が要求した情報を正常に受信したことは同値となる。したがって、情報提供者は正確かつ確実に情報を利用者に配送したことを確認できる。

【0180】また、上記の説明ではFiat Shamir 法をもとに説明したが、本方法は拡張FiatShamir 法 (太田一岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告 ISEC88-13) を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【0181】次に情報要求文 RS 、乱数文 Z 、検査文 e_i 、応答文 Y_i ($i = 1, 2, \dots, g$) からなる通信履歴 H の関係では、ゼロ知識証明プロトコルにおける検証式と第一および第二の一方方向性ランダムハッシュ関数とにより相互に関係し合っているため、一部を不正に改竄するなどして通信履歴 H を偽造することは不可能である。したがって、通信履歴 H を記録管理することによ

り、暗号文 C を復号して利用者が要求した情報 M を得ることができるための情報暗号化用秘密鍵 W_i ($i = 1, 2, \dots, g$) を利用者が確実に受信していることの証拠として、後日、調停者などの中立的な第三者に提示することができる。

【0182】以上の説明は、利用者が情報配送の要求を情報提供者に行い、情報提供者が要求された情報を正確かつ確実に利用者に配送したことを証明できるものであり、例えば情報 M を著作物などの有料情報とした場合、上記の情報配送方式によって情報提供者が利用者に情報 M を送信することにより、情報提供者が記録管理する通信履歴 H を著作権使用料等の情報料を徴収するときの証明情報として利用できるなど、様々な利用が可能である。

【0183】次に本発明の第8実施例について説明する。

【0184】図22は本発明の第8実施例における情報配送システムの構成を示すブロック図であり、10は利用者の端末 (端末) を示し、100から107までと109は第5の実施例と同様の構成であり、110は情報配送要求文を作成する入力手段、108は分割されたブロック情報を元の情報に再構成する情報再構成手段である。20は情報提供者 (端末) を示し、200から206までと209と210は第5実施例と同様の構成であり、208は後日、情報を利用者に配送した事実を証明する証拠としての通信履歴 H を記録管理する通信履歴ファイル、207は情報を任意ビット長の複数のブロックに分割し、蓄積する情報分割手段である。30は利用者と情報提供者とを通信で接続する通信回線を表す。40は調停者 (端末) を表し、401から403までは第7実施例と同様の構成であり、404は情報を任意ビット長の複数のブロックに分割し、蓄積する情報分割手段である。

【0185】以下、図23および図24のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を、また図25のフローチャートにしたがって調停での動作手順を説明する。

【0186】まず、準備段階として、信頼できるセンタが各利用者ごとに p_1, q_1, I, s を設定し、このうち N_1 と I を利用者の公開情報として公開し、 s を利用者の秘密情報として利用者秘密情報蓄積手段101に蓄積して利用者に秘密裏に配布する。ここで、 p_1 と q_1 は互いに異なる大きな素数を表し、 $N_1 = p_1 \times q_1$ である。また、 $I = s^2 \pmod{N_1}$ が成立している。

【0187】さらに、各情報提供者ごとに p, q, P, C, SC を設定し、このうち N, PC を情報提供者の公開情報 (公開鍵) として公開し、 SC を情報提供者の秘密情報 (秘密鍵) として情報提供者秘密情報蓄積手段201に蓄積して情報提供者に秘密裏に配布する。ここで、 p, q は互いに異なる大きな素数であり、 $N = p \times q$

である。また、 $PC \times SC = 1 \pmod{(p-1)(q-1)}$ が成立している。

【0188】(1) 情報配送ステップ

利用者は、情報提供者に提供して欲しい情報入力について入力手段110から情報配送要求文RSを作成し、一時メモリ102に蓄積した(S301)後、情報提供者の公開鍵PCを用いて公開鍵暗号手段107により暗号化情報配送要求文 $CR = RS^{PC} \pmod{N}$ に暗号化し

(S302)、通信回線30を介して情報提供者に送信する(S303)。ここで、情報配送要求文RSは、第7実施例と同じように、例えば要求日時、利用者識別番号、要求情報名、要求情報コード等から構成される。

【0189】情報提供者は、情報提供者秘密情報蓄積手段201に蓄積された秘密鍵SCを用いて、公開鍵暗号手段210により受信した暗号化情報配送要求文CRを情報配送要求文 $RS = CR^{SC} \pmod{N}$ に復号した後一時メモリ203に蓄積し(S304)、また乱数発生手段209により乱数文Zをランダムに生成した後一時メモリ203に蓄積する(S305)。

【0190】次に、情報配送要求文RSと乱数文Zとから演算手段204中の第一の方向性ランダムハッシュ関数f1によりgビットサイズの情報暗号化用秘密鍵 $W_i = f1(RS, Z)$ ($i=1, 2, \dots, g$)を生成して一時メモリ203に蓄積する(S306)。ここで、一般にgの値は共通鍵暗号手段105、205で使用する秘密鍵の鍵長と等しいかそれ以上である。その後、情報配送要求文RS中の要求情報コードをもとに、そのコードに対応する情報Mを情報データベース202から取り出し(S307)、情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を秘密鍵として共通鍵暗号手段205により暗号文 $C = E_i(M)$ に暗号化した(S308)後、利用者に暗号文Cを通信回線30を介して送信する(S309)。

【0191】利用者は、暗号文Cを情報蓄積手段109に受信/蓄積した後、受信した旨を通信回線30を介して情報提供者に通知する(S310)。

【0192】(2) 配送確認ステップ

情報提供者は、情報分割手段207において一時メモリ203に蓄積された情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を任意ビット長サイズの複数のブロックに

ここで、関数f3には例えば $V_{ij} = f3(W_{ij}, K_{ij}) = W_{ij} \oplus K_{ij}$ ($i=1, 2, \dots, L$)がある。なお、 \oplus は排他的論理和を表す。

利用者は、受信した検査文 e_{ij} ($i=1, 2, \dots, L$)を一時メモリ102に蓄積した(S319)後、演算手段104において検査文 e_{ij} のそれぞれのビットiに対し、一時メモリ102に蓄積された乱数 R_{ij} と利用者秘密情報蓄積手段101に蓄積された利用者の秘密情報sとから、 $e_{ij}=0$ ならば $Y_{ij}=R_{ij}$ を、 $e_{ij}=1$ ならば $Y_{ij}=s R_{ij} \pmod{N1}$ を計算し(S320)、応答

分割し、情報暗号化用ブロック秘密鍵として蓄積する(S311)。ここでは説明を簡単にするため、分割したブロック数をm、全てのブロックについてビット長をLで一定とし、分割した情報暗号化用秘密鍵を情報暗号化用ブロック秘密鍵 WB_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, m$)と表す。すなわち、 $WB_{ij} = W_{(i+(j-1)L)}$ であり、例えば $WB_{11}=W_1$ 、 $WB_{L1}=W_L$ 、 $WB_{12}=W_{L+1}$ 、 $WB_{Lm}=W_g$ のようになる。

【0193】これより以下の処理は第jブロックについてのものであり、配送確認ステップは第1ブロックから第mブロックまで各ブロックごとに以下の処理を順次(m回)繰り返す。

【0194】まず利用者は、乱数発生手段103によりL個の乱数 R_{ij} ($i=1, 2, \dots, L$)を生成した後一時メモリ102に蓄積し(S312)、それぞれについて演算手段104により初期応答文 $X_{ij} = R_{ij}^2 \pmod{N1}$ ($i=1, 2, \dots, L$)を計算した後一時メモリ102に蓄積し(S313)、初期応答文 X_{ij} ($i=1, 2, \dots, L$)を通信回線30を介して情報提供者に送信する(S314)。

【0195】情報提供者は、受信した初期応答文 X_{ij} ($i=1, 2, \dots, L$)を一時メモリ203に蓄積した(S315)後、一時メモリ203に蓄積された情報配送要求文RSと初期応答文 X_{ij} ($i=1, 2, \dots, L$)とから演算手段204中の第二の方向性ランダムハッシュ関数f2によりLビットサイズの鍵暗号化用秘密鍵 $K_{ij} = f2(RS, (X_{1j} \parallel X_{2j} \parallel \dots \parallel X_{Lj}))$ ($i=1, 2, \dots, L$)を生成して一時メモリ203に蓄積する(S316)。なお、f1とf2は同じ関数でも当然構わない。

【0196】次に、情報分割手段207に蓄積された第jブロック目の情報暗号化用ブロック秘密鍵 WB_{ij} ($i=1, 2, \dots, L$)と一時メモリ203に蓄積された鍵暗号化用秘密鍵 K_{ij} ($i=1, 2, \dots, L$)とから演算手段204中の第三の関数f3により秘密鍵配送文 V_{ij} ($i=1, 2, \dots, L$)を生成し、検査文 e_{ij} ($i=1, 2, \dots, L$)として一時メモリ203に蓄積した(S317)後、利用者に検査文 e_{ij} ($i=1, 2, \dots, L$)を通信回線30を介して送信する(S318)

【外3】

文 Y_{ij} ($i=1, 2, \dots, L$)として情報提供者に通信回線30を介して送信する(S321)。

【0197】情報提供者は、受信した応答文 Y_{ij} ($i=1, 2, \dots, L$)を一時メモリ203に蓄積した(S322)後、検証手段206において利用者の公開情報Iおよび一時メモリ203に蓄積された初期応答文 X_{ij} と応答文 Y_{ij} と検査文 e_{ij} とからそれぞれのビットiに対

し、 $e_{ij}=0$ ならば検証式 $Y_{ij}^2 = X_{ij} \pmod{N1}$ を、 $e_{ij}=1$ ならば検証式 $Y_{ij}^2 = X_{ij} \times I \pmod{N1}$ を満たすかどうかを検証する(S323)。この検証に失敗した場合には利用者は不正であるとみなして、ただちにプロトコルの実行を中止し(S324)、成功した場合にはすべてのブロックが終了するまで以上の処理を繰り返す(S325)。そして、第1ブロックから第mブロックまでの全てのブロックについて検証に成功した場合には、一時メモリ203に蓄積された情報配送要求文RS、乱数文Z、検査文 e_{ij} 、応答文 Y_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)を通信履歴Hとして通信履歴ファイル208に記録管理する(S326)。

【0198】(3) 情報取り出しステップ

利用者は、各ブロックについて一時メモリ102に蓄積された情報配送要求文RSと初期応答文 X_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)とから演算手段1

$$= V_{ij} \oplus K_{ij} \quad (i=1, 2, \dots, L: j=1, 2, \dots, m)$$

となる。なお、 \oplus は

排他的論理和を表す。

【0200】その後、情報再構成手段108により蓄積された情報暗号化用ブロック秘密鍵 WB_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)を用いて情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)に再構成して情報蓄積手段109に蓄積する(S330)。

【0201】最後に、情報蓄積手段109に蓄積された情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を秘密鍵として、共通暗号手段105により情報蓄積手段109に蓄積された暗号文Cを復号し(S331)、要求した情報 $M=D_c(C)$ を情報出力/利用手段106より獲得することができる(S332)。

(4) 調停

後日、利用者が要求した情報を受信していないと主張したり、情報配送の要求そのものを否定した場合には、情報提供者は通信履歴ファイル208に記録管理された通信履歴Hを提示し、調停者の一時メモリ402に蓄積する(S341)。

【0202】調停者は、演算手段401において利用者の公開情報Iと一時メモリ402に蓄積された通信履歴H中の検査文 e_{ij} および応答文 Y_{ij} からそれぞれのビットiに対し、 $e_{ij}=0$ ならば、 $X_{ij}=Y_{ij}^2 \pmod{N1}$ を $e_{ij}=1$ ならば $X_{ij}=Y_{ij}^2 / I \pmod{N1}$ を計算し、一時メモリ402に蓄積する(S342)。次に、一時メモリ402に蓄積された通信履歴H中の情報配送要求文RSと乱数文Zとから演算手段401中の第一の方向性ランダムハッシュ関数f1により情報暗号化用秘密鍵 $W_i = f1(RS, Z)$ ($i=1, 2, \dots, g$)を生成した(S343)後、情報分割手段404において情報暗号化用ブロック秘密鍵 WB_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)に分割して蓄積する

04中の第二の方向性ランダムハッシュ関数f2によりLビットサイズの鍵暗号化用秘密鍵 $K_{ij} = f2(RS, (X_{i1} \parallel X_{i2} \parallel \dots \parallel X_{ij}))$ ($i=1, 2, \dots, L: j=1, 2, \dots, m$)を生成し、一時メモリ102に蓄積する(S327)。

【0199】次に、一時メモリ102に蓄積された検査文 e_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)から秘密鍵配送文 V_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)を生成し、(S328)、生成した秘密鍵配送文 V_{ij} と鍵暗号化用秘密鍵 K_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)とから演算手段104中の第三の関数f3の逆関数f3'により情報暗号化用ブロック秘密鍵 WB_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)を取り出し、情報再構成手段108に蓄積する(S329)。ここで、例えば第三の関数f3の $V_{ij} = f3(W_{ij}, K_{ij})$

【外4】

(S344)。

【0203】各ブロック(第jブロック)について、一時メモリ402に蓄積された情報配送要求文RSと計算結果 X_{ij} ($i=1, 2, \dots, L$)とから演算手段401中の第二の方向性ランダムハッシュ関数f2により鍵暗号化用秘密鍵 $K_{ij} = f2(RS, (X_{i1} \parallel X_{i2} \parallel \dots \parallel X_{ij}))$ ($i=1, 2, \dots, L$)を生成して一時メモリ402に蓄積する(S345)。そして、情報分割手段404に蓄積された情報暗号化用ブロック秘密鍵 W_{ij} と一時メモリ402に蓄積された鍵暗号化用秘密鍵 K_{ij} ($i=1, 2, \dots, L$)とから演算手段401中の第三の関数f3により秘密鍵配送文 V_{ij} ($i=1, 2, \dots, L$)を生成し(S346)、検査文 e_{ij} ($i=1, 2, \dots, L$)として検証手段403において一時メモリ402に蓄積された通信履歴H中の検査文 e_{ij} ($i=1, 2, \dots, L$)と一致するかどうかを検査する(S347)。全てのブロック(第1ブロックから第mブロックまでのmブロック)について一致すれば(S348)、通信履歴Hの正当性が証明されたことになり(S349)、利用者が情報配送を要求し、かつ要求した情報を受信していることが保証される。そうでなければ通信履歴Hは無効とされる(S350)。

【0204】上記の情報配送方式を用いれば、第7実施例と同様の効果が得られるほかに、情報提供者と利用者の間で情報配送要求文RSについて暗号通信されているので、第三者が通信系列を盗聴したとしても、盗聴した通信系列からは情報配送要求文RSおよび鍵暗号化用秘密鍵 K_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)を求めることができない。また、情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)は検査文 e_{ij} と鍵暗号化用秘密鍵 K_{ij} ($i=1, 2, \dots, L: j=1, 2, \dots, m$)

とから求められることから、情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$) を第三者が求めることができないことと同値となるので、第三者が暗号文 C を復号し、不正に情報 M を獲得することを防止することが可能となる。

【0205】さらに、情報提供者と利用者との間の通信が情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$) の分割ブロック数 m と同じ回数だけ繰り返されるため、途中で情報提供者の検証に失敗した場合にはそれ以降の通信は打ち切れ、残りの検査文は送信されない。すなわち、利用者が知ることのできる検査文は検証に失敗する以前のもののみに限られるので、情報提供者の検証を失敗させた利用者は暗号文 C を復号するために必要な情報の一部しか獲得することができず、結果として正しい情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$) を生成することが不可能となる。

【0206】したがって、利用者の秘密情報 s を知らない不正な利用者が不正な応答文 Y_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, m$) を送信する場合はもとより、応答文そのものを送信しないような不正行為を行い、情報提供者が要求された情報 M を利用者に配送した事実を証明する通信履歴 H を情報提供者が記録管理できないにもかかわらず、利用者が要求した情報 M を獲得するのに必要な検査文 e_{ij} ($(i=1, 2, \dots, L; j=1, 2, \dots, m)$) を受信し、情報 M を不正に復号/獲得してしまうことがないようにすることが可能である。

【0207】また、上記の説明では分割するブロックを各ブロックともビット長を L で一定としたが、例えば第1ブロックは1ビット、第2ブロックは2ビット、第3ブロックは4ビットというようにブロックごとにビット長サイズを変えても当然構わない。

【0208】最後に、上記の説明における暗号通信のうち、公開鍵暗号方法による暗号通信については共通鍵暗号方法による暗号通信を行っても当然構わない。また、Fiat-Shamir 法をもとに説明をしたが、本方法は拡張 Fiat-Shamir 法 (太田一岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告 ISEC88-13) を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【0209】以上説明したとおり、本発明の第5～第8実施例によれば、ゼロ知識証明プロトコルを利用した情報配送方法では、第一に情報配送ステップにおいて、利用者が要求した情報は情報提供者によって暗号化されて利用者に配送されるため、この時点では要求した情報そのものを利用者が取り出すことはできない。第二に配送確認ステップで行われるプロトコル動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同じように不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。

第三に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了したことと同値であるから、情報提供者は利用者が検査文を正しく受信し、適正な処理をしていると判断できる。第四に情報取り出しステップにおいて、利用者は検査文を正しく受信できれば、秘密鍵配送文及び情報暗号化用秘密鍵を作成することができるので、この時点で前記情報暗号化用秘密鍵により暗号化された情報を復号し、要求した情報を取り出すことができる。したがって、これらの効果により、情報配送方法の全てのステップが終了した場合には、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は利用者が要求した情報を利用者まで確実に配送したと判断できる。

【0210】又、本発明の第5、第6実施例によれば、検査文について暗号通信をすることは、情報暗号化用秘密鍵についても暗号通信をしていることと同等の効果が得られることになり、第三者が通信路を盗聴したとしてもこれらの秘密鍵が知られることはない。さらに、情報暗号化用秘密鍵を解読するために有効な情報も得られないようにすることもできる。

【0211】又、本発明の第7、第8実施例によれば、情報提供者にとって都合のよい情報暗号化用秘密鍵を不正に作成できないようにすることができる。

【0212】又、通信履歴を偽造することは不可能であるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことを後日証明できる、証拠能力を持つことができる。

【0213】又、証拠能力を有する通信履歴を必要に応じて提示できるようになる。また、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井 (特開平5-12321) の方式と比較して大幅に削減できる。

【0214】又、情報提供者と利用者間で情報の提供の有無について調停をする必要が生じた場合、裁判所等の中立的な調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。

【0215】又、本発明の第8実施例によれば、情報配送要求文を暗号送信することにより、第三者による情報配送要求文の盗聴を防止し、どんな情報を要求したかなどの利用者のプライバシーが保護できる。

【0216】又、鍵暗号化用秘密鍵及び情報暗号化用秘密鍵については、情報提供者と利用者とのみの秘密の情報によりスクランブルされるので、第三者が通信路を盗聴したとしてもこれらの秘密鍵が知られることはなく、ま

た秘密鍵を解説するために有効な情報も得られない。したがって、利用者が要求した情報を第三者が不正に獲得することはできない。

【0217】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者へ送信されないことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として鍵暗号化用秘密鍵もしくは情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【0218】又、これらの実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【0219】又、情報暗号化秘密鍵を生成するときに乱数文を利用できるようにしたシステムとなる。

【0220】又、本発明の第5、第8実施例によれば、情報提供者が秘密に保持すべき情報を蓄積することができる情報提供者秘密情報蓄積手段を有したシステムとなる。

【0221】又、本発明の第5、第6、第8実施例によれば、情報提供者と利用者の間で公開鍵暗号方法による暗号通信ができるようにしたシステムとなる。

【0222】又、本発明の第7、第8実施例によれば、情報配送要求文を簡単に作成するための入力手段を利用者端末に備えたシステムとなる。

【0223】又、鍵暗号化用秘密鍵と秘密鍵配送文との生成機能を有し、情報暗号化用秘密鍵と鍵暗号用秘密鍵とを利用した情報配送ができるようにしたシステムとなる。

【0224】又、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【0225】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【0226】又、本発明の第8実施例によれば、不正な利用者があることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【0227】次に本発明の第9実施例について説明する。

【0228】図26は本発明の第9実施例における情報配送システムの構成を示すブロック図であり、10は情報の配送を受ける利用者（端末）を示し、100は通信

回線30を制御する通信制御手段、101は利用者の秘密情報を蓄積しておく利用者秘密情報蓄積手段、105は共通鍵暗号方法（例えば、DES、FEAL）を利用する共通鍵暗号手段、107は公開鍵暗号方法（例えば、RSA）を利用する公開鍵暗号手段、109は情報提供者からの配送された情報を蓄積する情報蓄積手段、102は利用者が必要な情報を一時的に蓄積する一時メモリ、103は利用者が乱数を生成するための乱数発生手段、104は必要な演算を行う演算手段、106は情報を出力もしくは利用する情報出力／利用手段である。20は情報を提供する情報提供者（端末）を示し、200は通信回線30を制御する通信制御手段、201は情報提供者の秘密情報を蓄積しておく情報提供者秘密情報蓄積手段、205は共通鍵暗号方法を利用する共通鍵暗号手段、210は公開鍵暗号方法を利用する公開鍵暗号手段、202は提供する情報が蓄積してある情報データベース、203は情報提供者が必要な情報を一時的に蓄積する一時メモリ、204は必要な演算を行う演算手段、206は情報の正当性を検証する検証手段、208は後日情報を利用者に配送した事実を証明する証拠としての通信履歴データHを記録管理する通信履歴ファイル、209は情報提供者が乱数を生成するための乱数発生手段である。30は利用者として情報提供者とを通信で接続する通信回線を表す。40は後日、情報提供者が通信履歴ファイル208に記録管理している通信履歴データHについて、中立的立場によりその通信履歴データHの正当性を判定する調停者（端末）を表し、402は調停者が必要な情報を一時的に蓄積する一時メモリ、405は公開鍵暗号方法を利用する公開鍵暗号手段、401は必要な演算を行う演算手段、403は正当性の判定を依頼された通信履歴データHについてその正当性を検証する検証手段である。

【0229】以下、図27および図28のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を、また図29のフローチャートにしたがって調停での動作手順を説明する。

【0230】なお、乱数Rと初期応答文Xと応答文Yを除くアルファベット文字は情報全体を表し、添え字付きアルファベット文字はその情報のビット情報を表す。例えば、情報暗号化用秘密鍵Wはgビット長で構成される情報暗号化用秘密鍵全体のことを表し、情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)は情報暗号化用秘密鍵の第iビット目のビット情報を表す。また、乱数Rと初期応答文Xと応答文Yの添え字は複数個生成される同一種類の情報の中のひとつの情報を表す。例えば、乱数 R_i ($i=1, 2, \dots, g$)はg個生成される乱数の中の第i番目に生成された乱数情報であることを表す。

【0231】(0)準備段階

信頼できるセンタが各利用者ごとに $p_1, q_1, ID, S, p_2, q_2, PU, SU$ を設定し、このうちN1,

$N2$, ID , PU を利用者の公開情報として公開し、 S , SU を利用者の秘密情報として利用者秘密情報蓄積手段101に蓄積して利用者に秘密裏に配布する。ここで、 $(p1, q1)$ と $(p2, q2)$ の各組はそれぞれ互いに異なる大きな素数の組になっており、 $N1 = p1 \times q1$, $N2 = p2 \times q2$ である。また、 $ID = S^2 \pmod{N1}$, $PU \times SU = 1 \pmod{(p2-1)(q2-1)}$ が成立している。なお、 $p1 = p2$, $q1 = q2$ としてもよい。

【0232】さらに、各情報提供者ごとに p , q , PC , SC を設定し、このうち N , PC を情報提供者の公開鍵として公開し、 SC を情報提供者の秘密鍵として情報提供者秘密情報蓄積手段201に蓄積して情報提供者に秘密裏に配布する。ここで、 p , q は互いに異なる大きな素数であり、 $N = pq$ である。また $PC \times SC = 1 \pmod{(p-1)(q-1)}$ が成立している。

【0233】(1) 情報配送ステップ

情報提供者は、乱数発生手段209で g ビット長の情報暗号化用秘密鍵 W を任意に生成して一時メモリ203に蓄積する(S361)。ここで、一般に g の値は共通鍵暗号手段105と205で使用する秘密鍵の鍵長と等しいかそれ以上である。後に、情報 M を情報データベース202から取り出し(S362)、情報暗号化用秘密鍵 W を秘密鍵として共通鍵暗号手段205により暗号文 $C = E(M)$ に暗号化した(S363)後、利用者に暗号文 C を通信回線30を介して送信する(S364)。

【0234】利用者は、暗号文 C を情報蓄積手段109に受信/蓄積した後、受信した旨を通信回線30を介して情報提供者に通知する(S365)。

【0235】なお、ここではS364の暗号文 C の送信について通信回線30を使用しているが、もちろんCD-ROMなどの物理媒体に記録して、通信回線を使用せずに一般に配布するようにしても構わない。その場合には、S365の動作は省略されることが多い。

【0236】(2) 配送確認ステップ

情報提供者は、公開鍵暗号手段210により情報暗号化用秘密鍵 W を情報提供者の公開鍵 PC で暗号化し(S366)、暗号化した情報暗号化用秘密鍵 $CW = W^{PC} \pmod{N}$ を利用者に通信回線30を介して通信する(S367)。

【0237】利用者は、公開鍵暗号手段107により利用者の秘密情報 SU を用いて暗号化された情報暗号化用

$$K_{ij} = W_{ij} \oplus K_{ij} \quad (i = 1, 2, \dots, L : j = 1, 2, \dots, b) \text{ がある。}$$

なお、 \oplus は排他的論理和を表す。

これより以下の処理は第 j ブロックについてのものであり、配送確認ステップは第1ブロックから第 b ブロックまで各ブロックごとに以下の処理を順次(b 回)繰り返す行なう。

秘密鍵 CW にデジタル署名を行い(S368)、署名付き情報暗号化用秘密鍵 $SW = CW^{SU} \pmod{N2}$ を通信回線30を介して情報提供者に送信する(S369)。

【0238】情報提供者は、署名付き情報暗号化用秘密鍵 SW を一時メモリ203に蓄積した(S370)後、検証手段206において利用者の公開鍵 PU を用いて署名検証式 $CW = SW^{PU} \pmod{N2}$ を満たすかどうかを検証する(S371)。この検証に失敗した場合には利用者は不正であると見做してただちにプロトコルの実行を中止する(S372)。また検証に成功した場合には、演算手段204において情報暗号化用秘密鍵 W を任意ビット長の複数のブロックに分割し、情報暗号化用ブロック秘密鍵 WB を生成する(S373)。ここでは説明を簡単にするため、分割したブロック数を b 、全てのブロックについてビット長を L で一定とし、分割した情報暗号化用秘密鍵を情報暗号化用ブロック秘密鍵 WB_{ij} ($i = 1, 2, \dots, L : j = 1, 2, \dots, b$)と表す。すなわち、 $WB_{ij} = W_{(i+L(j-1))}$ であり、例えば $WB_{11} = W_1$, $W_{11} = W_L$, $WB_{12} = W_{L+1}$, $WB_{1b} = W_g$ のようになる。

【0239】利用者は、乱数発生手段103により g 個の乱数 R_{ij} ($i = 1, 2, \dots, L : j = 1, 2, \dots, b$)を生成した後一時メモリ102に蓄積し(S374)、それぞれについて演算手段104により初期応答文 $X_{ij} = R_{ij}^2 \pmod{N1}$ ($i = 1, 2, \dots, L : j = 1, 2, \dots, b$)を計算した後一時メモリ102に蓄積し(S375)、初期応答文 X_{ij} ($i = 1, 2, \dots, L : j = 1, 2, \dots, b$)を通信回線30を介して情報提供者に送信する(S376)。

【0240】情報提供者は、初期応答文 X_{ij} ($i = 1, 2, \dots, L : j = 1, 2, \dots, b$)を一時メモリ203に蓄積した(S377)後、演算手段204中の一方方向性ランダムハッシュ関数 $h(\cdot)$ により g ビット長の鍵暗号化用秘密鍵 $K_{ij} = h(X_{ij} \| X_{2j} \| \dots \| X_{Lj})$ ($i = 1, 2, \dots, L : j = 1, 2, \dots, b$)を生成し(S378)、情報暗号化用ブロック秘密鍵 WB_{ij} と鍵暗号化用秘密鍵 K_{ij} ($i = 1, 2, \dots, L : j = 1, 2, \dots, b$)とから演算手段204中の関数 $f(\cdot)$ により検査文 e_{ij} ($i = 1, 2, \dots, L : j = 1, 2, \dots, b$)を生成して一時メモリ203に蓄積する(S379)。ここで、関数 f には例えば $e_{ij} = f(W$

【外5】

【0241】情報提供者は、利用者に検査文 e_{ij} ($i = 1, 2, \dots, L$)を通信回線30を介して送信する(S380)。

【0242】利用者は、検査文 e_{ij} ($i = 1, 2, \dots,$

L)を一時メモリ102に蓄積した(S381)後、演算手段104において検査文 e_{ij} のそれぞれのビット i に対し、乱数 R_{ij} と利用者の秘密情報 S とから、 $e_{ij}=0$ ならば $Y_{ij}=R_{ij}$ を、 $e_{ij}=1$ ならば $Y_{ij}=S \times R_{ij} \pmod{N1}$ を計算し(S382)、応答文 Y_{ij} ($i=1, 2, \dots, L$)として情報提供者に通信回線30を介して送信する(S383)。

【0243】情報提供者は、応答文 Y_{ij} ($i=1, 2, \dots, L$)を一時メモリ203に蓄積した(S384)後、検証手段206において利用者の公開情報ID、初期応答文 X_{ij} 、応答文 Y_{ij} および検査文 e_{ij} とからそれぞれのビット i に対し、 $e_{ij}=0$ ならば検証式 $Y_{ij}^2 = X_{ij} \pmod{N1}$ を、 $e_{ij}=1$ ならば検証式 $Y_{ij}^2 = X_{ij} \times ID \pmod{N1}$ を満たすかどうかを検証する(S385)。この検証に失敗した場合には利用者は不正であると見做して直ちにプロトコルの実行を中止し(S386)、また成功した場合にはS380に戻り、すべてのブロックが終了するまで以上の処理を繰り返す(S387)。そして、第1ブロックから第 b ブロックまでの

数 $f(\cdot)$ の $e_{ij} = f(W_{ij}, K_{ij}) = W_{ij} \oplus K_{ij}$ ($i=1, 2, \dots, L; j=1, 2, \dots, b$)に対し、逆関数 $f'(\cdot)$ は $W_{ij} = f'(e_{ij}, K_{ij}) = e_{ij} \oplus K_{ij}$ ($i=1, 2, \dots, L; j=1, 2, \dots, b$)となる。なお、 \oplus は排他的

論理和を表す。その後、演算手段104に情報暗号化用ブロック秘密鍵 WB_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$)を用いて情報暗号化用秘密鍵 W_i ($i=1, 2, \dots, g$)を生成し、情報蓄積手段109に蓄積する(S391)。最後に、情報暗号化用秘密鍵 W を秘密鍵として共通暗号手段105により情報蓄積手段109に蓄積された暗号文 C を復号し(S392)、情報 $M=D, (C)$ を情報出力/利用手段106より獲得することができる(S393)。

【0245】(4) 調停

後日、利用者が情報を受信していないと主張した場合には、情報提供者は通信履歴ファイル208に記録管理された通信履歴データ H を提示し、調停者の一時メモリ402に蓄積する(S401)。

【0246】調停者は、公開暗号手段405において情報暗号化用秘密鍵 W を情報提供者の公開鍵 PC で暗号化した情報暗号化用秘密鍵 $CW=W^P \pmod{N}$ を生成し(S402)、検証手段403において署名付き情報暗号化用秘密鍵 SW が利用者の公開鍵 PU を用いて署名検証式 $CW=SW^U \pmod{N2}$ を満たすかどうかを検証する。(S403)。検証が失敗した時は通信履歴データ H は無効とされる(S404)。

【0247】署名の検証が成功した場合には、演算手段401において利用者の公開情報IDと通信履歴データ H 中の検査文 e_{ij} および応答文 Y_{ij} からそれぞれのビッ

全てのブロックについて検証に成功した場合には、情報暗号化用秘密鍵 W 、署名付き情報暗号化用秘密鍵 SW 、検査文 e_{ij} 、応答文 Y_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$)を通信履歴データ H として通信履歴ファイル208に記録管理する(S388)。

【0244】(3) 情報取り出しステップ

利用者は、初期応答文 X_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$)から演算手段104中の一方向性ランダムハッシュ関数 $h(\cdot)$ により g ビット長の鍵暗号化用秘密鍵 $K_{ij}=h(X_{ij} \parallel X_{2j} \parallel \dots \parallel X_{Lj})$ ($i=1, 2, \dots, L; j=1, 2, \dots, b$)を生成し(S389)、検査文 e_{ij} と鍵暗号化用秘密鍵 K_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$)とから演算手段104中の関数 $f(\cdot)$ の逆関数 $f'(\cdot)$ により情報暗号化用ブロック秘密鍵 WB_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$)を取り出す(S390)。ここで、例えば関

【外6】

ト i に対し、 $e_{ij}=0$ ならば、 $X_{ij}=Y_{ij}^2 \pmod{N1}$ を、 $e_{ij}=1$ ならば $X_{ij}=Y_{ij}^2 / ID \pmod{N1}$ を計算して一時メモリ402に蓄積し(S405)、情報暗号化用秘密鍵 W から演算手段401において情報暗号化用ブロック秘密鍵 WB_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$)を生成する(S406)。次に、計算結果 X_{ij} ($i=1, 2, \dots, L$)から演算手段401中の一方向性ランダムハッシュ関数 $h(\cdot)$ により g ビット長の鍵暗号化用秘密鍵 $K_{ij}=h(X_{ij} \parallel X_{2j} \parallel \dots \parallel X_{Lj})$ ($i=1, 2, \dots, L; j=1, 2, \dots, b$)を生成し(S407)、情報暗号化用ブロック秘密鍵 WB_{ij} と鍵暗号化用秘密鍵 K_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$)とから演算手段401中の関数 $f(\cdot)$ により検査文 e_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$)を生成して(S408)、検証手段403において一時メモリ402に蓄積された通信履歴データ H 中の検査文 e_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$)と全てのビットについて一致するかどうかを検査する(S409)。全てのビットについて一致すれば、通信履歴データ H の正当性が証明されたことになり、利用者が情報 M を受信していることが保証される(S410)。そうでなければ通信履歴データ H は無効とされる(S411)。

【0248】上記の情報配送方式を用いれば、情報 M は初めに暗号文 C に暗号化されて利用者へ送信もしくは物

理媒体により配布されるため、暗号文Cを利用者が入手した時点では情報Mを獲得されることはない。そしてプロトコルが正常に終了した時点で、ゼロ知識証明プロトコルによる利用者認証が正常に行なわれたことのほかに、検査文eを利用者が正常に受信したことが確認できる。また、検査文eの他は利用者自身が作成した初期応答文 X_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$) から情報暗号化用秘密鍵Wを生成し、利用者が暗号文Cを復号して情報Mを獲得することができるため、検査文eを利用者が正常に受信したと利用者が情報Mを正常に受信したことは同値となる。したがって、情報提供者は正確かつ確実に情報Mを利用者に配送したことを確認できる。

【0249】また、情報提供者と利用者との間の通信は情報暗号化用秘密鍵Wの分割ブロック数bと同じ回数だけ繰り返行なわれるため、途中で情報提供者の検証に失敗した場合にはそれ以降の通信は打ち切れ、残りの検査文は送信されない。すなわち、利用者が知ることのできる検査文は検証に失敗する以前のもののみに限られるので、情報提供者の検証を失敗させた利用者は暗号文Cを復号するために必要な情報の一部しか獲得することができず、結果として正しい情報暗号化用秘密鍵Wを生成することが不可能となる。したがって、利用者の秘密情報Sを知らない不正な利用者が不正な応答文を送信する場合はもとより、応答文そのものを送信しないような不正行為を行ない、情報提供者が情報Mを利用者に配送した事実を証明する通信履歴データHを情報提供者が記録できないにも関わらず、利用者が情報Mを獲得するのに必要な検査文eを全て受信し、情報Mを不正に復号/獲得してしまうことがないようにすることが可能である。なお、上記の説明では分割するブロックを各ブロックともビット長をLで一定としたが、例えば第1ブロックは1ビット、第2ブロックは2ビット、第3ブロックは4ビットというようにブロックごとにビット長を変えても当然構わない。

【0250】次に、署名付き情報暗号化用秘密鍵SWは利用者にしか作成できないため、情報暗号化秘密鍵Wもしくは署名付き情報暗号化用秘密鍵SWを情報提供者が不正に改変することはできない。また、情報暗号化用秘密鍵Wと、初期応答文 X_{ij} 、検査文 e_{ij} 、応答文 Y_{ij} ($i=1, 2, \dots, L; j=1, 2, \dots, b$) からなる通信系列との関係では、ゼロ知識証明プロトコルにおける検証式と一方向性ランダムハッシュ関数 $h(\cdot)$ とにより相互に関係し合っているため、それらの一部を不正に改変するなどして通信系列を改変・偽造することは不可能である。したがって、通信履歴データHを記録保管することにより暗号文Cを復号して利用者が情報Mを獲得できるための情報暗号化用秘密鍵Wを利用者が確実に受信していることの証拠として後に調停者などの中立的な第三者に提示することができる。

【0251】以上の説明は、情報提供者が情報Mを正確かつ確実に利用者に配送したことを証明できるものであり、例えば情報Mを著作物などの有料情報とした場合、上記の情報配送方法によって情報提供者が利用者に情報Mを送信することにより、情報提供者が記録管理する通信履歴データHを著作権使用料等の情報料を徴収するときの証明情報として利用できるなど、様々な利用が可能である。

【0252】また、上記の説明ではFiat Shamir 法をもとに説明をしたが、本方法は拡張Fiat Shamir 法(太田・岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告 ISEC88-13)を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【0253】以上説明したとおり、本発明の第9実施例によれば、ゼロ知識証明プロトコルを利用した情報配送方法では、第一に情報配送ステップにおいて、利用者が要求した情報は情報提供者によって暗号化されて利用者に配送されるため、この時点では要求した情報そのものを利用者が取り出すことはできない。第二に配送確認ステップで行われるプロトコル動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同じように不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第三に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了したと同値であるから、情報提供者は利用者が検査文を正しく受信し、適正な処理をしていると判断できる。第四に情報取り出しステップにおいて、利用者は検査文を正しく受信できれば情報暗号化用秘密鍵を作成することができるので、この時点で前記情報暗号化用秘密鍵により暗号化された情報を復号し、要求した情報を取り出すことができる。したがって、これらの効果により、情報配送方法の全てのステップが終了した場合には、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は利用者が要求した情報を利用者まで確実に配送したと判断できる。

【0254】又、情報提供者が自分に都合のよい情報暗号化用秘密鍵に不正に改竄できないようにすることができる。さらに、暗号化された情報暗号化用秘密鍵は情報提供者以外は復号することができないので、署名を行う時点では利用者に情報暗号化用秘密鍵を知られることはない。

【0255】又、通信履歴を偽造することは不可能であるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送

し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【0256】又、証拠能力を有する通信履歴を必要に応じて提示できるようになる。また、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平 5 - 1 2 3 2 1）の方式と比較して大幅に削減できる。

【0257】又、情報提供者と利用者の間で情報の提供の有無について調停をする必要が生じた場合、裁判所等の中立的な調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。

【0258】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者へ送信されないことになる。したがって、情報提供者の検証に失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【0259】又、この実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【0260】又、情報暗号化秘密鍵を生成するときに乱数文を利用できるようにしたシステムとなる。

【0261】又、情報提供者が秘密に保持すべき情報を蓄積することができる情報提供者秘密情報蓄積手段を有したシステムとなる。

【0262】又、情報提供者と利用者の間で公開鍵暗号方法による暗号通信ができるようにしたシステムとなる。

【0263】又、鍵暗号化用秘密鍵と生成機能を有し、情報暗号化用秘密鍵と鍵暗号化用秘密鍵とを利用した情報配送ができるようにしたシステムとなる。

【0264】又、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【0265】又、裁判所等の中立的な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【0266】又、不正な利用者があることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【0267】尚、本発明は上述した各実施例に限定され

るものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【0268】

【発明の効果】以上説明したとおり、上記第 1 実施例では、第一に情報提供者による利用者の認証方法としてゼロ知識証明プロトコルを利用しているため、ゼロ知識証明プロトコルの目的や従来からの利用方法からいっても、利用者が正当なカードを利用していなければ情報提供者の検証をクリアし続けることはほとんど不可能であり、認証段階でほぼ完全に拒絶される。

【0269】第二に情報提供者から配送情報を利用者へ配送する部分では、配送情報をゼロ知識証明プロトコルの検査文に含めて配送を行なっているため、ゼロ知識証明プロトコルが正常に終了すれば、カード上において間違いなく検査文、すなわち配送情報を受信・記録し、適正な処理をしていたことになる。また、途中で情報提供者の検証に失敗した場合にはそれ以降の認証は打ち切れ、残りの検査文は配送されないため、利用者が知ることのできる配送情報は検証に失敗する以前のものに限られる。

【0270】第三に通信履歴（前記 X_i 、前記 Y_i 、前記検査文 e_{ji} ）を記録管理することにより情報提供者と利用者との間で正常な認証が行なわれたことを情報提供者は確認できるので、第二の効果と合わせて利用者は配送情報を受信し、かつカードの蓄積手段 14 に配送情報が記録されているはずである。このことは、情報提供者から開示される通信履歴と利用者から提出されるカードに記録された配送情報とを照合することによって、利用者が情報暗号化用秘密鍵 W を生成できる状態であるかどうかを判定できる。なお、この場合、利用者からカードの提出がない場合には、情報暗号化用秘密鍵 W は生成できる状態にあると判定する。

【0271】したがって、不正な利用者がシステムを利用したり、あるいは配送情報のすべてを不正に搾取したりすることはできない。また、正常に認証が終了しているにも関わらず利用者が配送情報を受信していないなどという不当な主張に対して、情報提供者は通信履歴を開示するとともに、利用者にカードを提出するよう要求することにより対抗できる。

【0272】また、上記第 1 実施例において、配送情報すべてを分割して検査文 e_{ji} を生成する必要性はなく、例えば、配送情報の始めから gn ビット目までを検査文 e_{ji} ($j = 1, \dots, n$) とし、 n 組の検査文 e_{ji} によるゼロ知識証明プロトコルが終了した後、配送情報の残りの部分を一括して送信するような情報の配送方法とすれば、 n の値を様々に変えることにより、ゼロ知識証明におけるセキュリティレベルを変えられるうえ、通信量を削減できる。例えば n を L/g の半分とすれば、通信量もほぼ半分となる。

【0273】また、検査文 e_{ji} の生成方法についても、

単純に配送情報を分割して生成するだけでなく、ダミー情報を付加したり、あるいは暗号化を行ったりして生成することも可能である。この場合、カード内にあらかじめ設定されている秘密情報、もしくは蓄積された検査文 e_{ji} から自律的にダミー情報を除去、あるいは復号を行ったりして元の配送情報に復元する機能を持たせることにより、ゼロ知識証明を正常に終了しないかぎり、前記配送情報を取り出せないようにできる。したがって、第三者もしくは利用者が検査文 e_{ji} を不正に搾取したり、大部分の検査文 e_{ji} を受信した後、故意に認証を失敗させ、検査文 e_{ji} のうち配送されてこない残りの部分を予測したりする等の不正行為を行ない、情報提供者が配送に失敗したと判断あるいは気がつかないうちに、第三者もしくは利用者が配送情報を獲得してしまうことがないようにできる。

【0274】また、上記第1実施例による情報配送方法およびシステムでは、ゼロ知識証明プロトコルに必要な情報はすべて耐タンパー装置上に組み込まれており、実際の情報配送においても耐タンパー装置上に組み込まれた手段のみを用いて実行されるため、前記情報が外部に漏れることはなく、たとえカード所有者であっても前記情報を知ることができない。したがって、カード自体を偽造したり、あるいはカード上の記録情報を書き換えたりする等の不正行為を防止できる。

【0275】一方、上記第2～第4実施例のゼロ知識証明プロトコルを利用した情報配送方法では、第一にプロトコルの動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同様に、不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第二に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了した事実と同値であるので、情報提供者は正しい利用者が情報を正しく受信していると判断できる。

【0276】又、情報を暗号化し暗号文として送信することにより、第三者による情報の盗聴を防止し、かつ第三者が情報を解読するために有効な情報も得られないようにすることもできる。

【0277】又、上記第2実施例によれば、暗号文の復号処理を配送確認ステップと切り離して実行することができる。

【0278】又、上記第2、第3実施例によれば、例えばハッシュ関数などを用いて情報（または利用者が復号可能な暗号文）から検査文を生成することにより検査文のサイズを小さくすることができ、配送確認ステップにおける通信量及び処理時間を削減できる。

【0279】又、上記第3実施例によれば、一方向性関数を用いて検査文を生成することにより、情報（または利用者が復号可能な暗号文）、応答文、及び検査文とからなる通信履歴の偽造を不可能にする。

【0280】又、例えば不正な利用者による利用などに

より配送確認ステップの途中で情報提供者のプロトコルに失敗した場合には、直ちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者へ送信されないことになるため、結果として情報（または利用者が復号可能な暗号文）全てを不正に獲得してしまうことがないようにできる。

【0281】又、上記第4実施例によれば、大容量の情報を送信する場合に、第一に情報は情報提供者が生成した情報暗号化用秘密鍵によって初めに暗号化されて利用者へ配送されるため、利用者の認証が行われる以前に情報本体を利用者が取り出すことはできない。第二に情報暗号化用秘密鍵についてのみ検査文として配送確認を行うことにより、通信量及び配送確認のための処理時間を大幅に短縮できる。第三に配送確認ステップが正常に終了すれば利用者は検査文を正しく受信したことが確認でき、情報取り出しステップにおいて情報暗号化用秘密鍵を獲得することが保証されるので、この時点で初めて情報を間違いなく取り出すことができる。したがって、これらの効果により情報配送方法が終了した場合には、情報提供者は正規の利用者に対して情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者へ配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は情報を利用者まで確実に配送したと判断できる。

【0282】又、一方向性関数を用いて情報暗号化用秘密鍵を生成することにより情報提供者にとって都合の良い情報暗号化用秘密鍵を不正に生成できないようにすることができる。また、同様に一方向性関数を用いることにより、乱数文と検査文と応答文とからなる通信履歴を偽造することは不可能になるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者へ配送し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【0283】又、検査文について暗号通信を行うことは、情報暗号化用秘密鍵についても暗号通信を行なっていることと同等の効果が得られるため、第三者による情報暗号化用秘密鍵の盗聴を防止し、かつ第三者が情報暗号化用秘密鍵を解読するために有効な情報も得られないようになる。

【0284】又、検査文の復号処理を配送確認ステップと切り離して実行することができる。

【0285】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者へ送信されないことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として情報本体もしくは情報暗号化用秘密鍵を生成することが不可能

となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【0286】又、上記第3、第4実施例によれば、偽造不可能な通信履歴を実際に情報を配送した証拠として記録管理することができ、かつ必要に応じて提示できるようになる。さらに、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平5-12321）の方式と比較して大幅に削減できる。

【0287】又、情報提供者と利用者の間で情報の提供の有無について調停を行う必要が生じた場合、情報提供者が通信履歴を裁判所等の中立な調停機関に提示し、調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。すなわち、情報提供者が利用者に対して情報（または利用者が復号可能な暗号文）を送信し、かつ利用者が確実に受信したことを、後日調停者が確認できるので、利用者が情報（または利用者が復号可能な暗号文）を受信しているにも関わらず、利用者が情報を受信していないなどという不当な主張を防止できる。

【0288】又、上記第2～第4実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【0289】又、情報提供者と利用者の間で暗号通信ができるようにしたシステムとなる。

【0290】又、上記第4実施例によれば、情報提供者から提供された情報を蓄積し、利用者が必要に応じて情報を利用できるようにしたシステムとなる。

【0291】又、情報暗号化用秘密鍵の生成機能を有し、情報暗号化用秘密鍵を用いた情報配送ができようにしたシステムとなる。

【0292】又、上記第3、第4実施例によれば、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【0293】又、不正な利用者であることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【0294】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定できるようにしたシステムとなる。

【0295】一方、上記第5～第8実施例によれば、ゼロ知識証明プロトコルを利用した情報配送方法では、第一に情報配送ステップにおいて、利用者が要求した情報は情報提供者によって暗号化されて利用者に配送される

ため、この時点では要求した情報そのものを利用者が取り出すことはできない。第二に配送確認ステップで行われるプロトコル動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同じように不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第三に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了した事実と同値であるから、情報提供者は利用者が検査文を正しく受信し、適正な処理をしていると判断できる。第四に情報取り出しステップにおいて、利用者は検査文を正しく受信できれば、秘密鍵配送文及び情報暗号化用秘密鍵を作成することができるので、この時点で前記情報暗号化用秘密鍵により暗号化された情報を復号し、要求した情報を取り出すことができる。したがって、これらの効果により、情報配送方法の全てのステップが終了した場合には、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は利用者が要求した情報を利用者まで確実に配送したと判断できる。

【0296】又、上記第5、第6実施例によれば、検査文について暗号通信をすることは、情報暗号化用秘密鍵についても暗号通信をしていることと同等の効果が得られることになり、第三者が通信路を盗聴したとしてもこれらの秘密鍵が知られることはない。さらに、情報暗号化用秘密鍵を解読するために有効な情報も得られないようにすることもできる。

【0297】又、上記第7、第8実施例によれば、情報提供者にとって都合のよい情報暗号化用秘密鍵を不正に作成できないようにすることができる。

【0298】又、通信履歴を偽造することは不可能であるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【0299】又、証拠能力を有する通信履歴を必要に応じて提示できるようになる。また、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平5-12321）の方式と比較して大幅に削減できる。

【0300】又、情報提供者と利用者の間で情報の提供の有無について調停をする必要が生じた場合、裁判所等の中立な調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。

【0301】又、上記第8実施例によれば、情報配送要求文を暗号送信することにより、第三者による情報配送要求文の盗聴を防止し、どんな情報を要求したかなどの

利用者のプライバシーが保護できる。

【0302】又、鍵暗号化用秘密鍵及び情報暗号化用秘密鍵については、情報提供者と利用者のみの秘密の情報によりスクランブルされるので、第三者が通信路を盗聴したとしてもこれらの秘密鍵が知られることはなく、また秘密鍵を解読するために有効な情報も得られない。したがって、利用者が要求した情報を第三者が不正に獲得することはできない。

【0303】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者には送信されないことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として鍵暗号化用秘密鍵もしくは情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【0304】又、上記第5～第8実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【0305】又、情報暗号化秘密鍵を生成するときに乱数文を利用できるようにしたシステムとなる。

【0306】又、上記第5、第8実施例によれば、情報提供者が秘密に保持すべき情報を蓄積することができる情報提供者秘密情報蓄積手段を有したシステムとなる。

【0307】又、上記第5、第6、第8実施例によれば、情報提供者と利用者の間で公開鍵暗号方法による暗号通信ができるようにしたシステムとなる。

【0308】又、上記第7、第8実施例によれば、情報配送要求文を簡単に作成するための入力手段を利用者端末に備えたシステムとなる。

【0309】又、鍵暗号化用秘密鍵と秘密鍵配送文との生成機能を有し、情報暗号化用秘密鍵と鍵暗号用秘密鍵とを利用した情報配送ができるようにしたシステムとなる。

【0310】又、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【0311】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【0312】又、上記第8実施例によれば、不正な利用者があることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【0313】一方、上記第9実施例によれば、ゼロ知識

証明プロトコルを利用した情報配送方法では、第一に情報配送ステップにおいて、利用者が要求した情報は情報提供者によって暗号化されて利用者に配送されるため、この時点では要求した情報そのものを利用者が取り出すことはできない。第二に配送確認ステップで行われるプロトコル動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同じように不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第三に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了した事実と同値であるから、情報提供者は利用者が検査文を正しく受信し、適正な処理をしていると判断できる。第四に情報取り出しステップにおいて、利用者は検査文を正しく受信できれば情報暗号化用秘密鍵を作成することができるので、この時点で前記情報暗号化用秘密鍵により暗号化された情報を復号し、要求した情報を取り出すことができる。したがって、これらの効果により、情報配送方法の全てのステップが終了した場合には、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は利用者が要求した情報を利用者まで確実に配送したと判断できる。

【0314】又、情報提供者が自分に都合のよい情報暗号化用秘密鍵に不正に改竄できないようにすることができる。さらに、暗号化された情報暗号化用秘密鍵は情報提供者以外は復号することができないので、署名を行う時点では利用者に情報暗号化用秘密鍵を知られることはない。

【0315】又、通信履歴を偽造することは不可能であるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【0316】又、証拠能力を有する通信履歴を必要に応じて提示できるようになる。また、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平5-12321）の方式と比較して大幅に削減できる。

【0317】又、情報提供者と利用者の間で情報の提供の有無について調停をする必要が生じた場合、裁判所等の中立な調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。

【0318】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者には送信されない

ことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【0319】又、上記第9実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【0320】又、情報暗号化秘密鍵を生成するときに乱数文を利用できるようにしたシステムとなる。

【0321】又、情報提供者が秘密に保持すべき情報を蓄積することができる情報提供者秘密情報蓄積手段を有したシステムとなる。

【0322】又、情報提供者と利用者の間で公開鍵暗号方法による暗号通信ができるようにしたシステムとなる。

【0323】又、鍵暗号化用秘密鍵と生成機能を有し、情報暗号化用秘密鍵と鍵暗号用秘密鍵とを利用した情報配送ができるようにしたシステムとなる。

【0324】又、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【0325】又、裁判所等の中立的な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【0326】又、不正な利用者があることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【図面の簡単な説明】

【図1】従来のFiat Shamir 法による利用者認証方式と、従来の認証方式によるメッセージ認証方式と、従来のRSA署名法によるデジタル署名方式を示す概念図である。

【図2】本発明の第1実施例における情報配送システムの構成例を示すブロック図である。

【図3】図2に示す情報配送システムの動作手順を示すフローチャートである。

【図4】図2に示す情報配送システムで用いる配送情報の例を示す模式図である。

【図5】本発明の第2実施例における情報配送システムの構成例を示すブロック図である。

【図6】図5に示す情報配送システムの動作手順を示すフローチャートである。

【図7】本発明の第3実施例における情報配送システムの構成例を示すブロック図である。

【図8】図7に示す情報配送システムの配送確認に関する動作手順を示すフローチャートである。

【図9】図7に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

【図10】本発明の第4実施例における情報配送システムの構成例を示すブロック図である。

【図11】図10に示す情報配送システムの配送確認と情報取り出しに関する動作手順を示すフローチャートである。

【図12】図10に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

【図13】本発明の第5実施例における情報配送システムの構成例を示すブロック図である。

【図14】図13に示す情報配送システムの動作手順を示すフローチャートである。

【図15】本発明の第6実施例における情報配送システムの構成例を示すブロック図である。

【図16】図15に示す情報配送システムの動作手順を示すフローチャートである。

【図17】本発明の第7実施例における情報配送システムの構成例を示すブロック図である。

【図18】図17に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順を示すフローチャートである。

【図19】図17に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

【図20】図17に示す情報配送システムで用いる情報配送要求文の構成形態を示す模式図である。

【図21】図17に示す情報配送システムで用いる通信履歴の構成形態を示す模式図である。

【図22】本発明の第8実施例における情報配送システムの構成例を示すブロック図である。

【図23】図22に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順の前半を示すフローチャートである。

【図24】図22に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順の後半を示すフローチャートである。

【図25】図22に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

【図26】本発明の第9実施例における情報配送システムの構成例を示すブロック図である。

【図27】図26に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順の前半を示すフローチャートである。

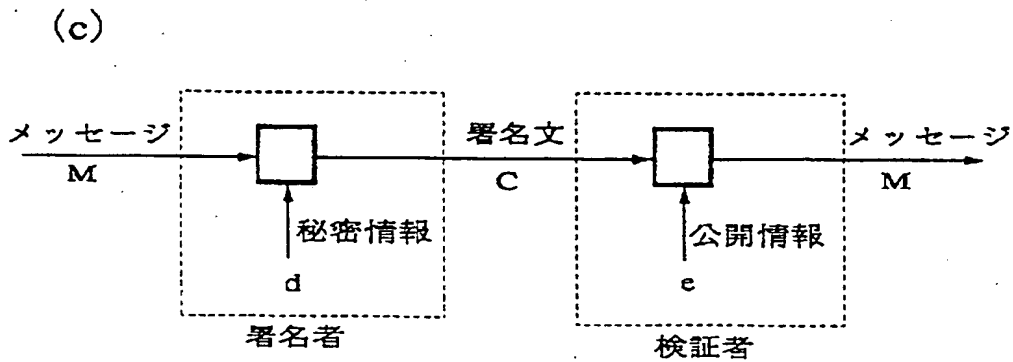
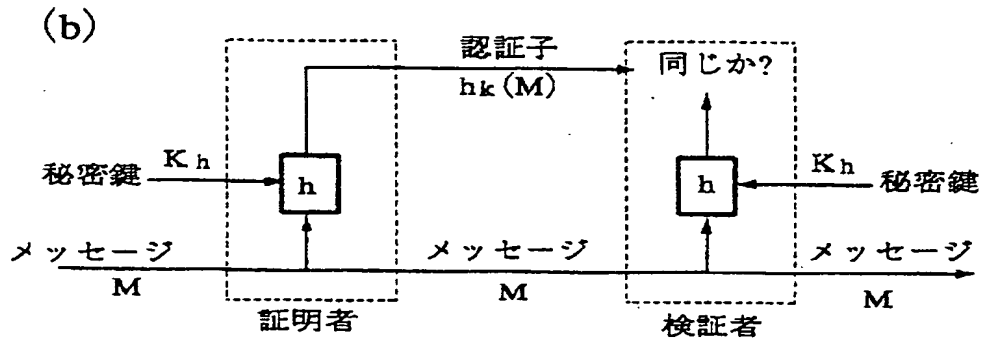
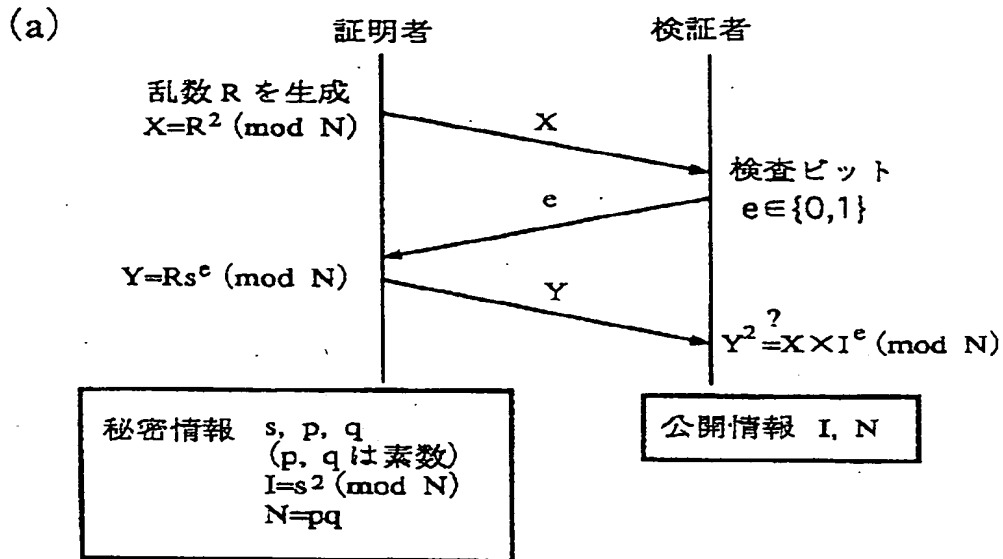
【図28】図26に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順の後半を示すフローチャートである。

【図29】図26に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

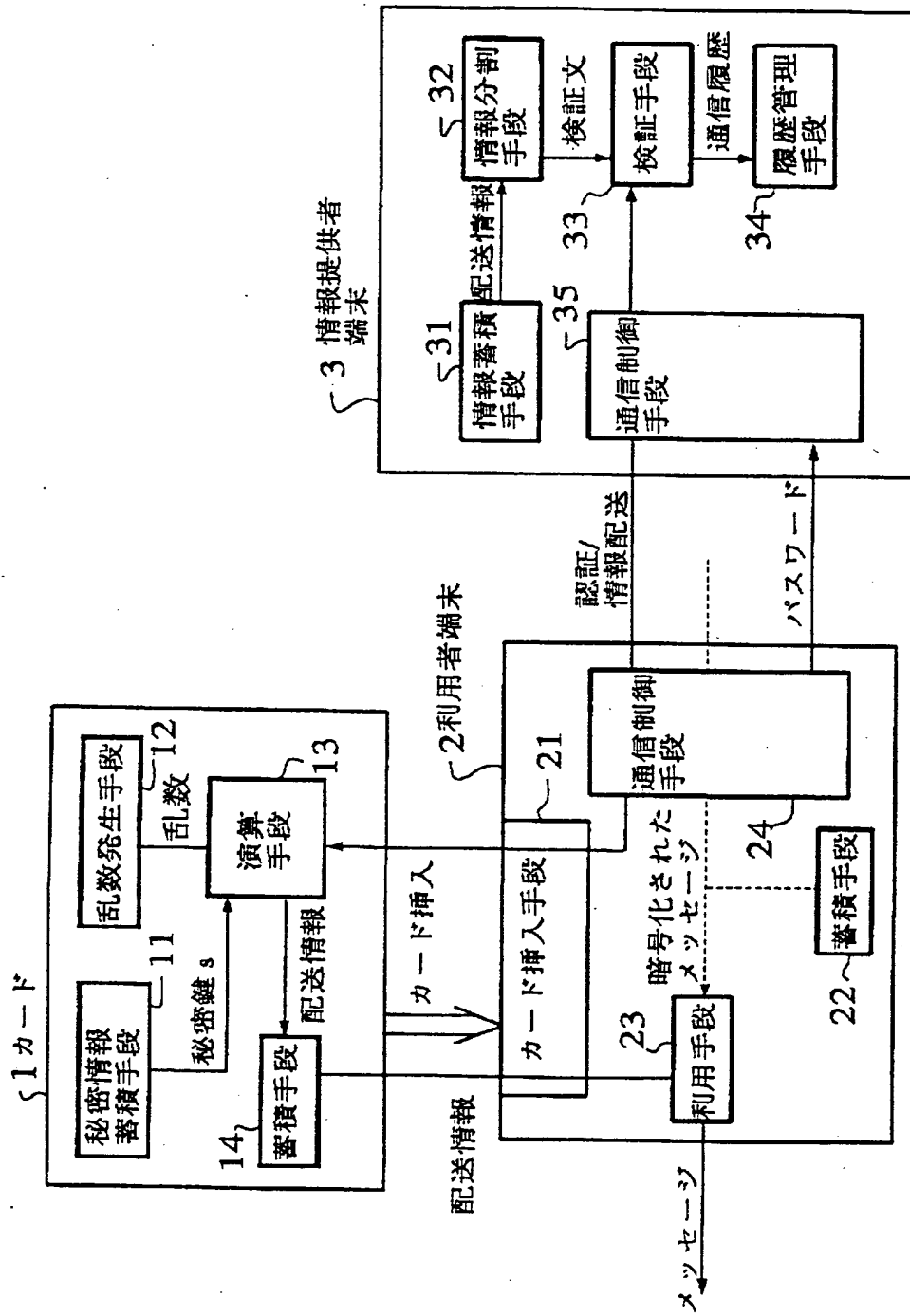
【符号の説明】

- 1 カード
 - 1 1 秘密情報蓄積手段
 - 1 2 乱数発生手段
 - 1 3 演算手段
 - 1 4 蓄積手段
- 2 利用者端末
 - 2 1 カード挿入手段
 - 2 2 蓄積手段
 - 2 3 利用手段
 - 2 4 通信制御手段
- 3 情報提供者端末
 - 3 1 情報蓄積手段
 - 3 2 情報分割手段
 - 3 3 検証手段
 - 3 4 履歴管理手段
 - 3 5 通信制御手段
- 5 0 配送情報
- 1 0 利用者端末
- 2 0 情報提供者端末
- 3 0 通信回線
- 4 0 調停者端末
- 1 0 0 通信制御手段
- 1 0 1 利用者秘密情報蓄積手段
- 1 0 2 一時メモリ
- 1 0 3 乱数発生手段
- 1 0 4 演算手段
- 1 0 5 共通鍵暗号手段
- 1 0 6 情報出力／利用手段
- 1 0 7 公開鍵暗号手段
- 1 0 8 情報再構成手段
- 1 0 9 情報蓄積手段
- 1 1 0 入力手段
- 4 1 演算手段
- 4 2 一時メモリ
- 4 3 検証手段
- 4 4 情報分割手段
- 4 5 公開鍵暗号手段
- 2 0 0 通信制御手段
- 2 0 1 情報提供者秘密情報蓄積手段
- 2 0 2 情報データベース
- 2 0 3 一時メモリ
- 2 0 4 演算手段
- 2 0 5 共通鍵暗号手段
- 2 0 6 検証手段
- 2 0 7 情報分割手段
- 2 0 8 通信履歴ファイル
- 2 0 9 乱数発生手段
- 2 1 0 公開鍵暗号手段
- 4 0 1 演算手段
- 4 0 2 一時メモリ
- 4 0 3 検証手段
- 4 0 4 情報分割手段
- 4 0 5 公開鍵暗号手段

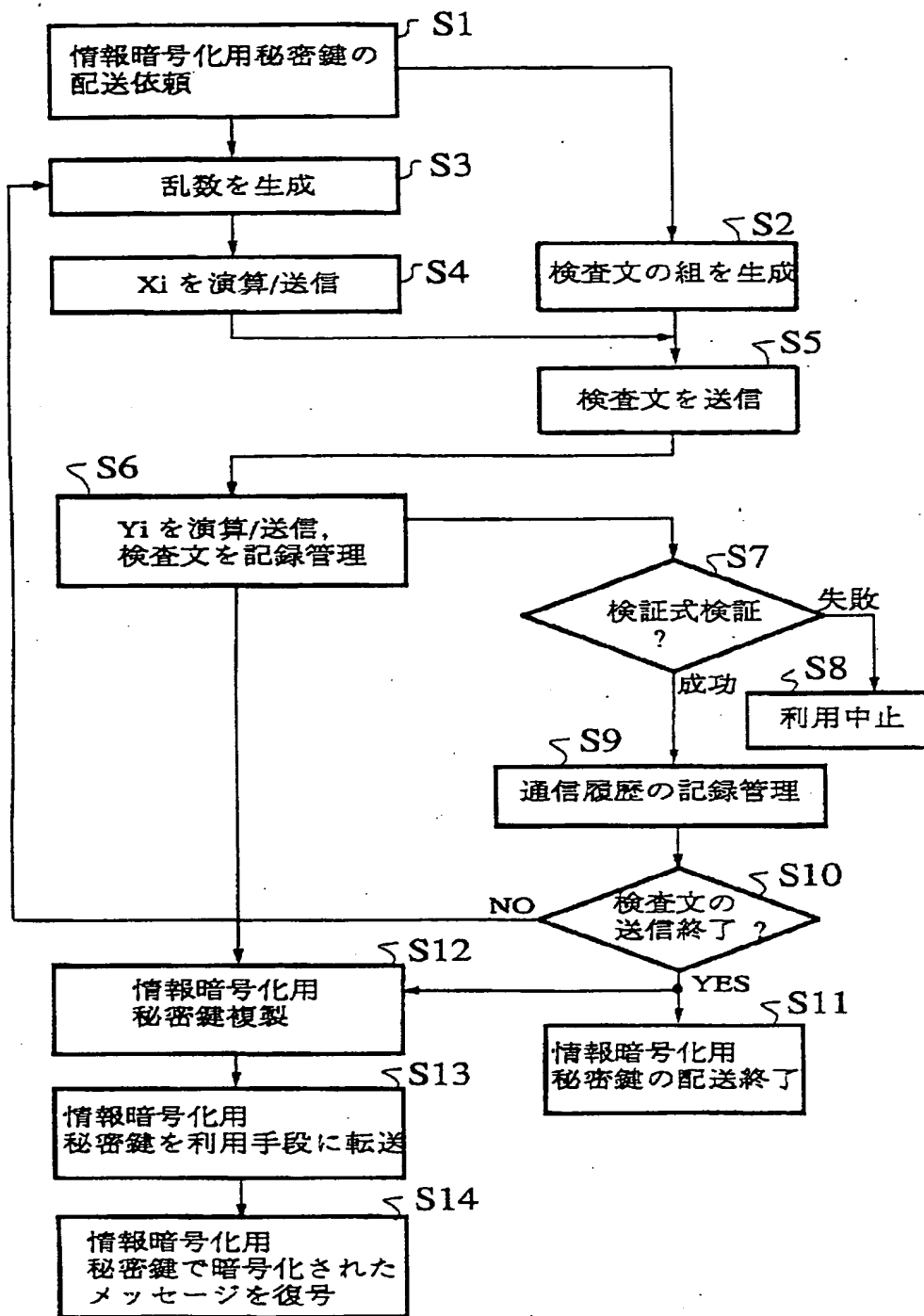
【図1】



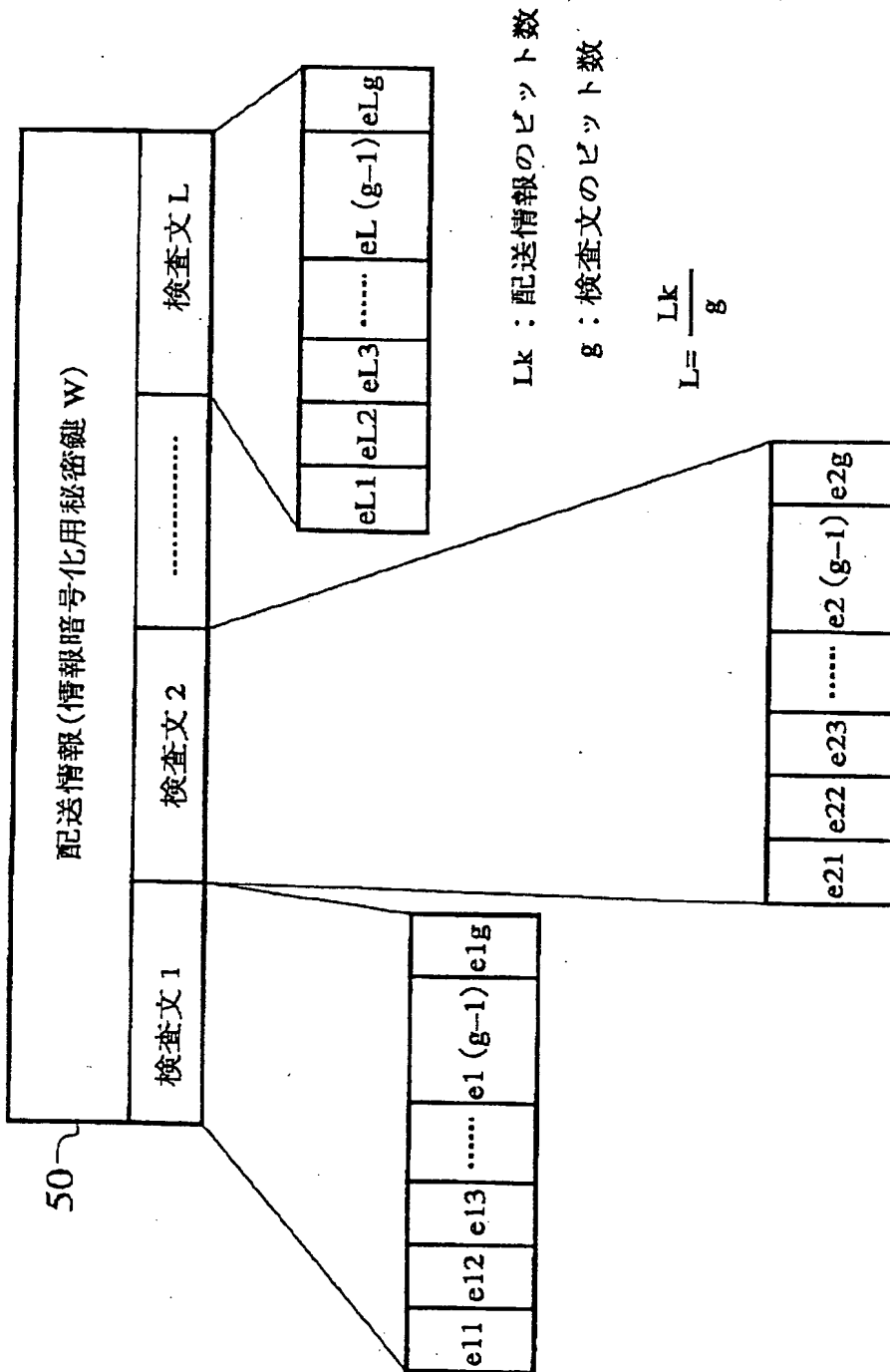
[図2]



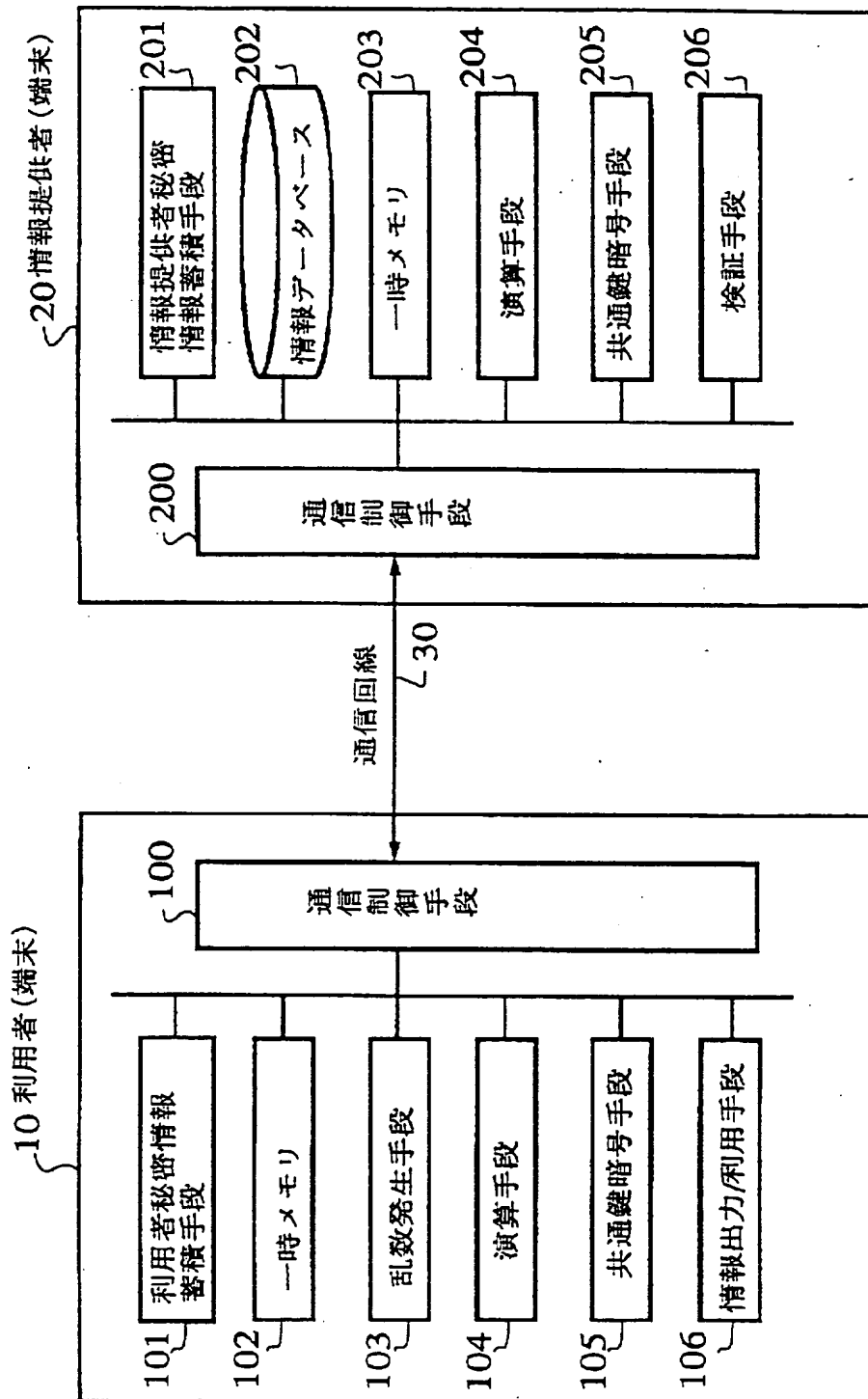
【図 3】



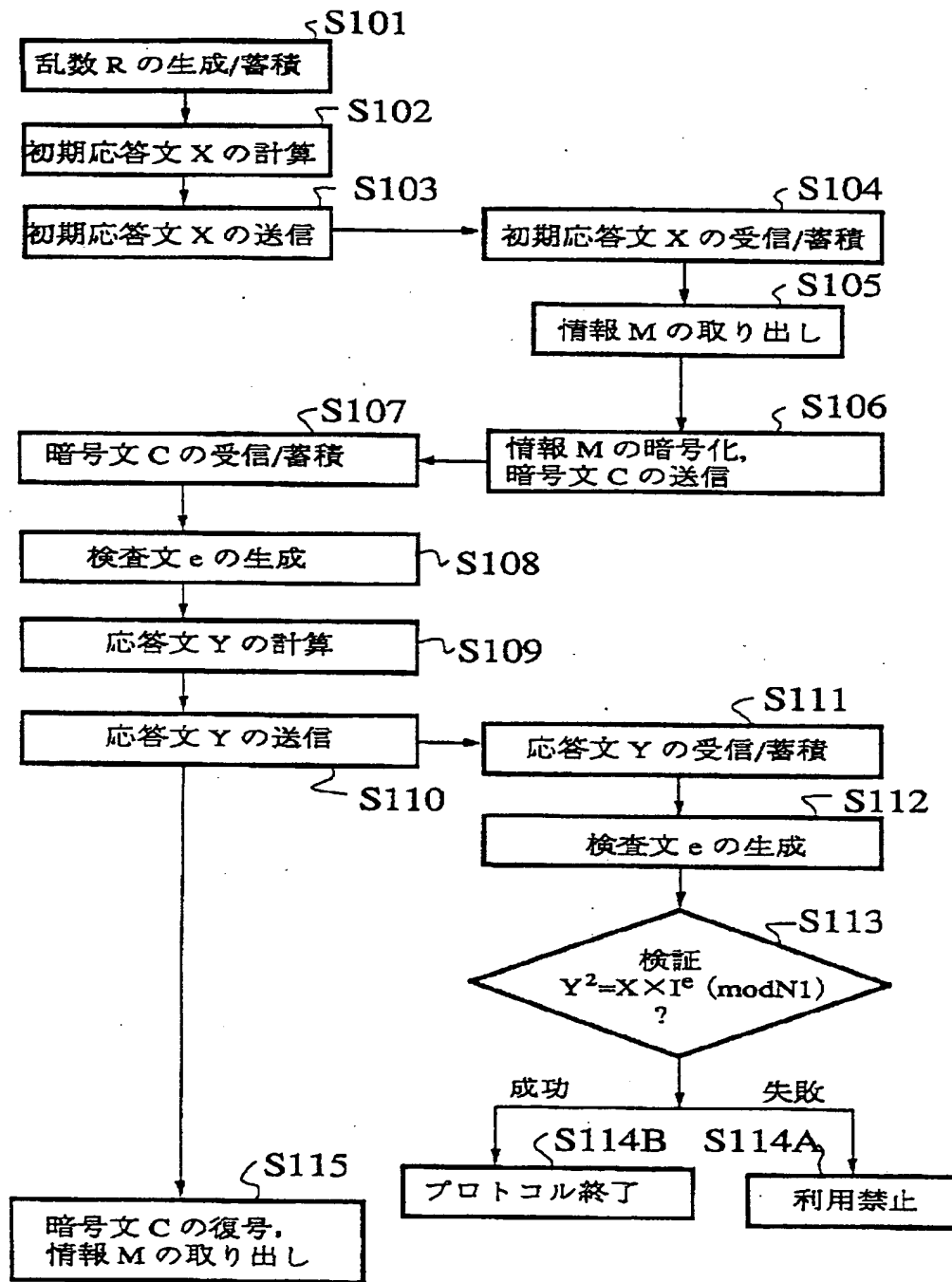
【図4】



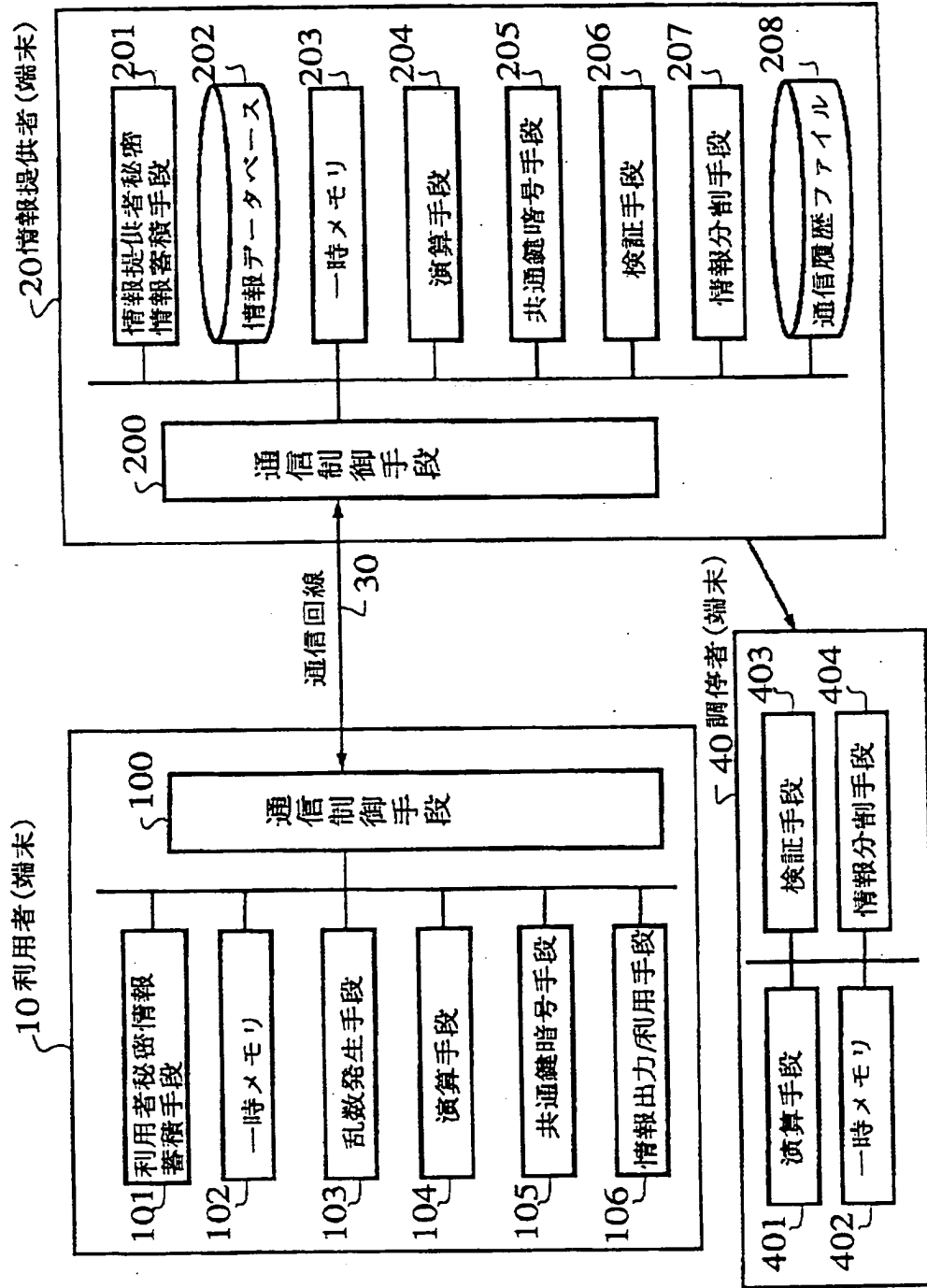
【図5】



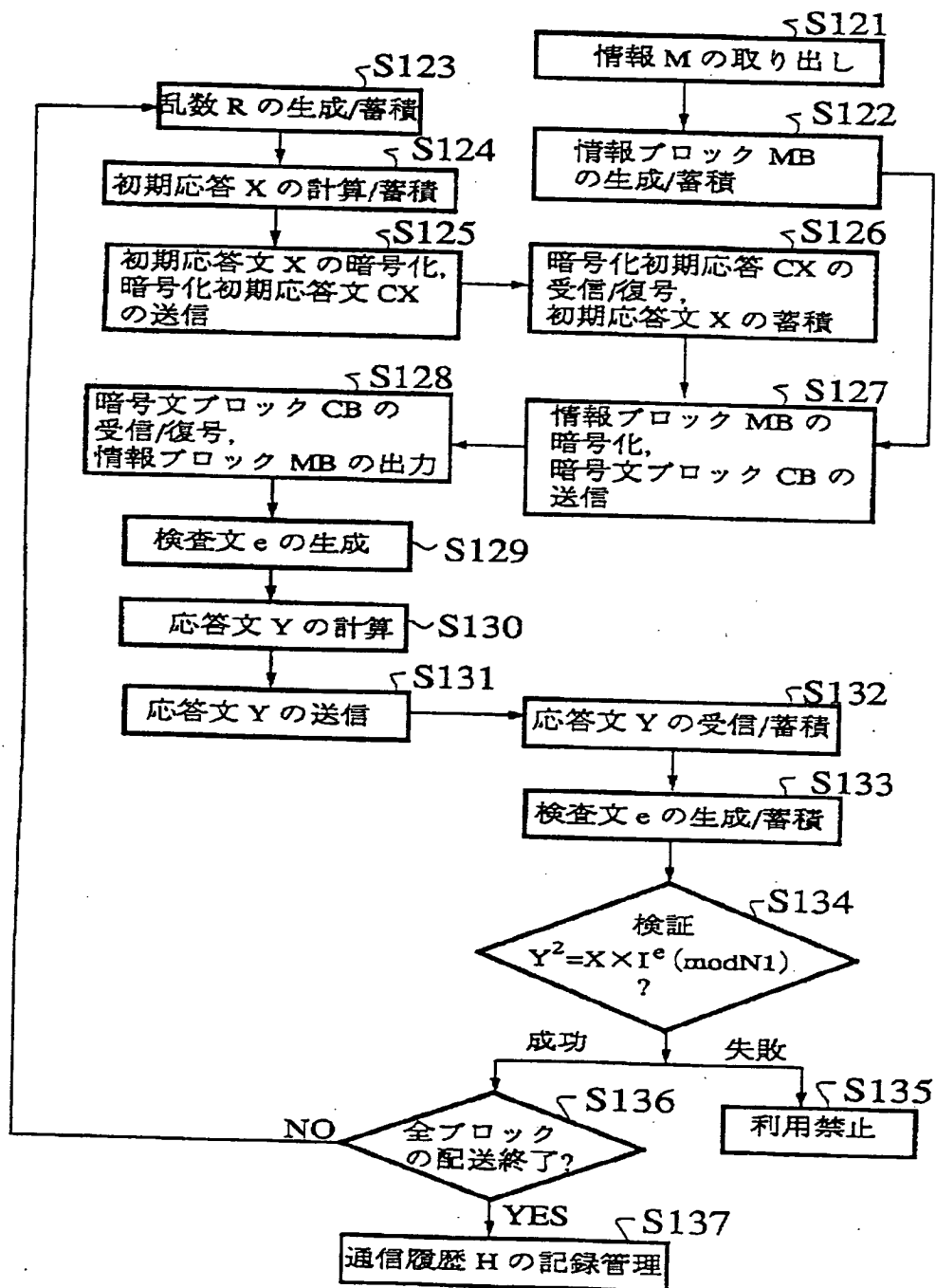
【図 6】



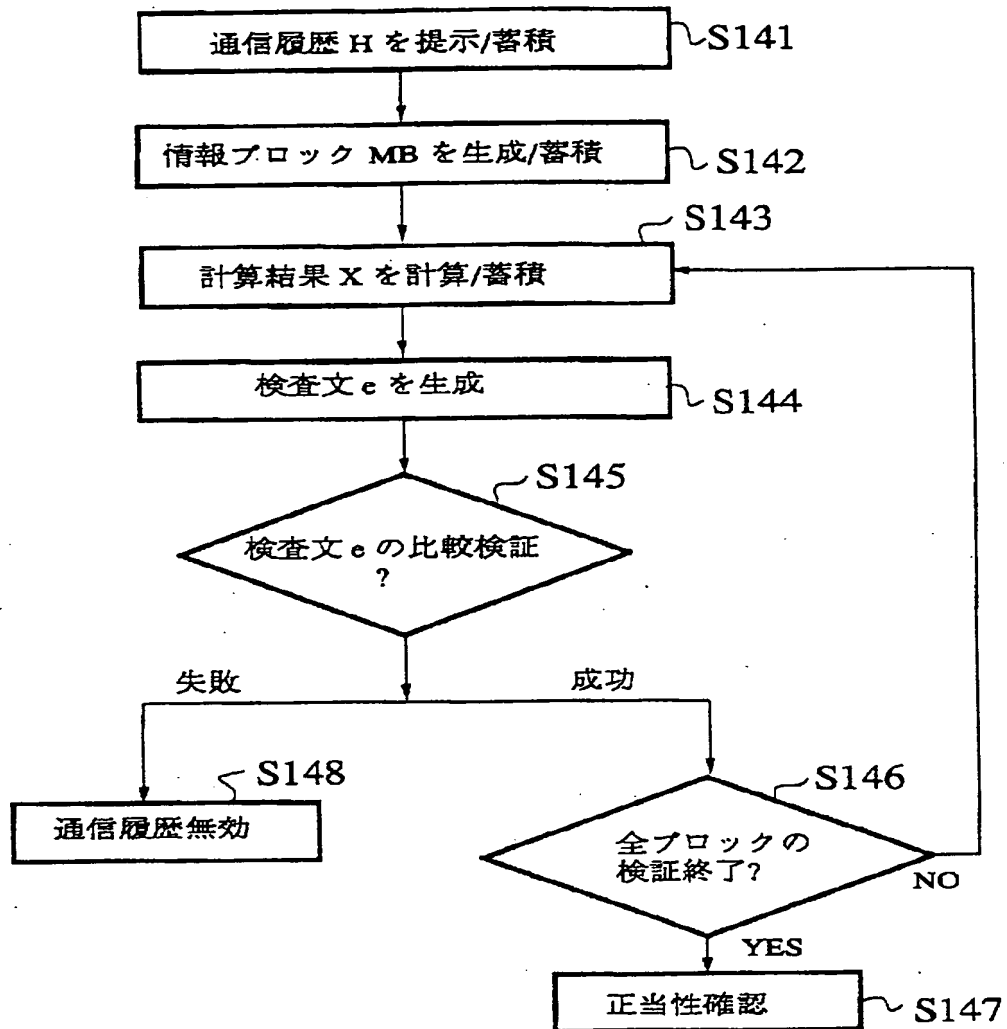
【図7】



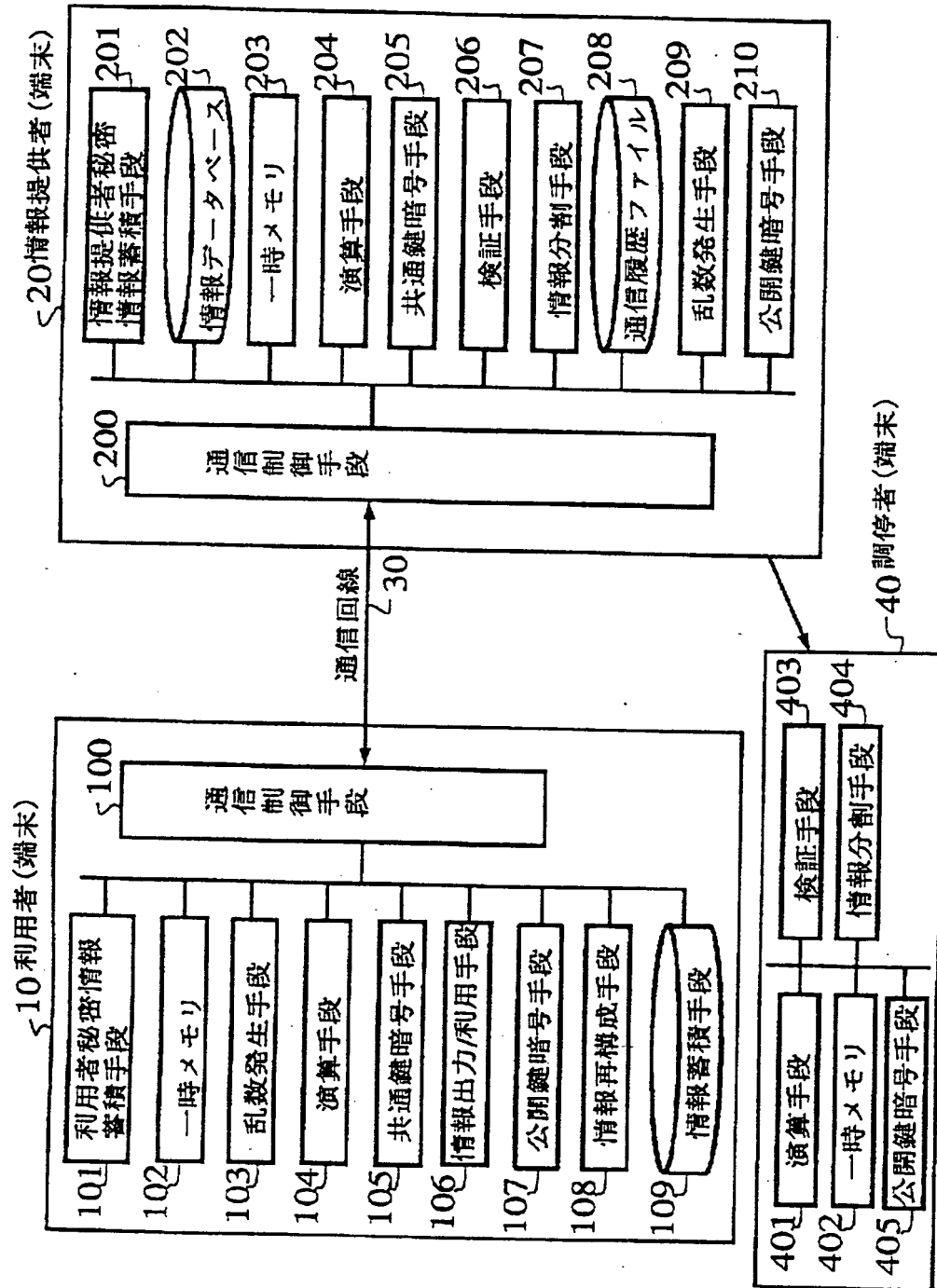
【図8】



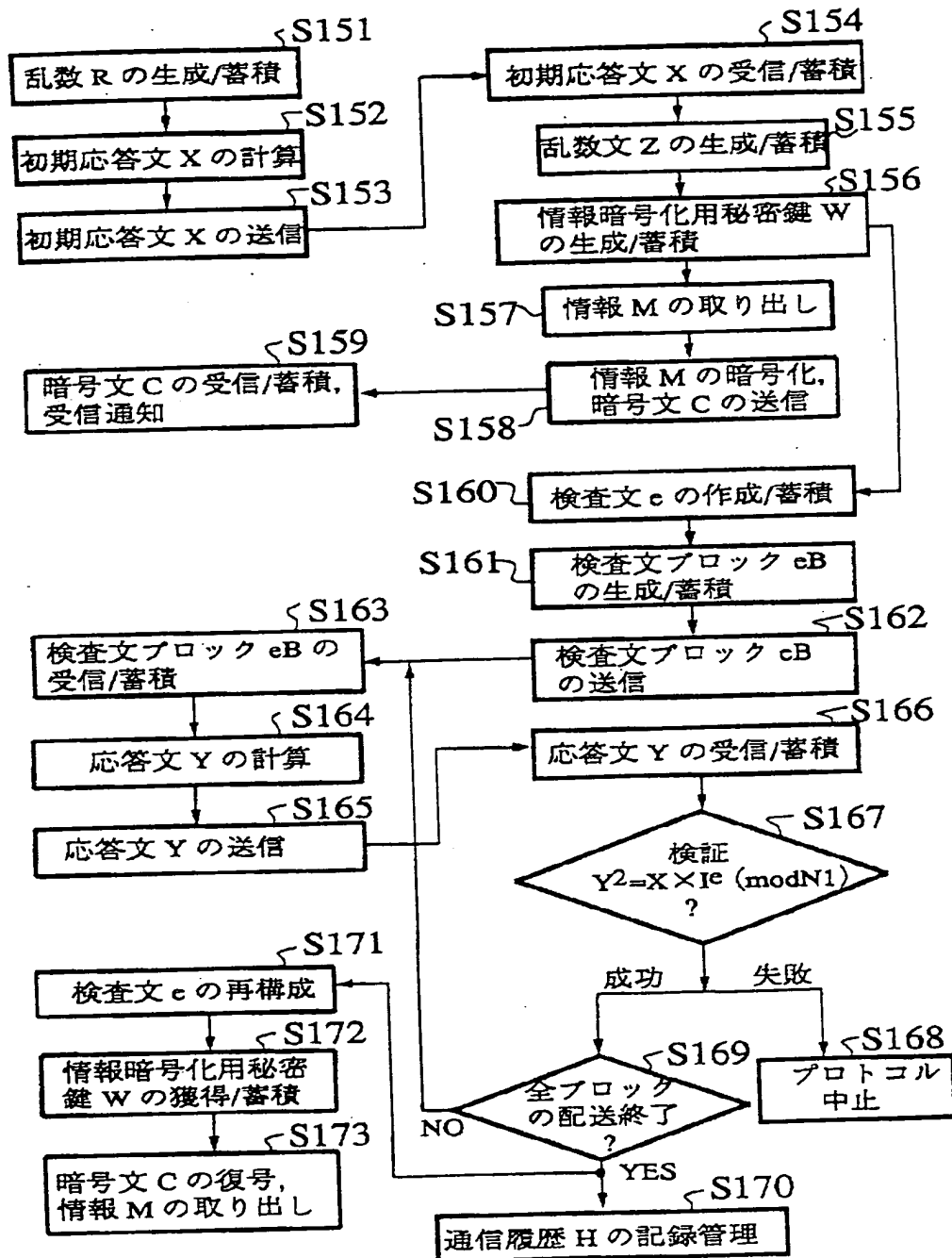
【図 9】



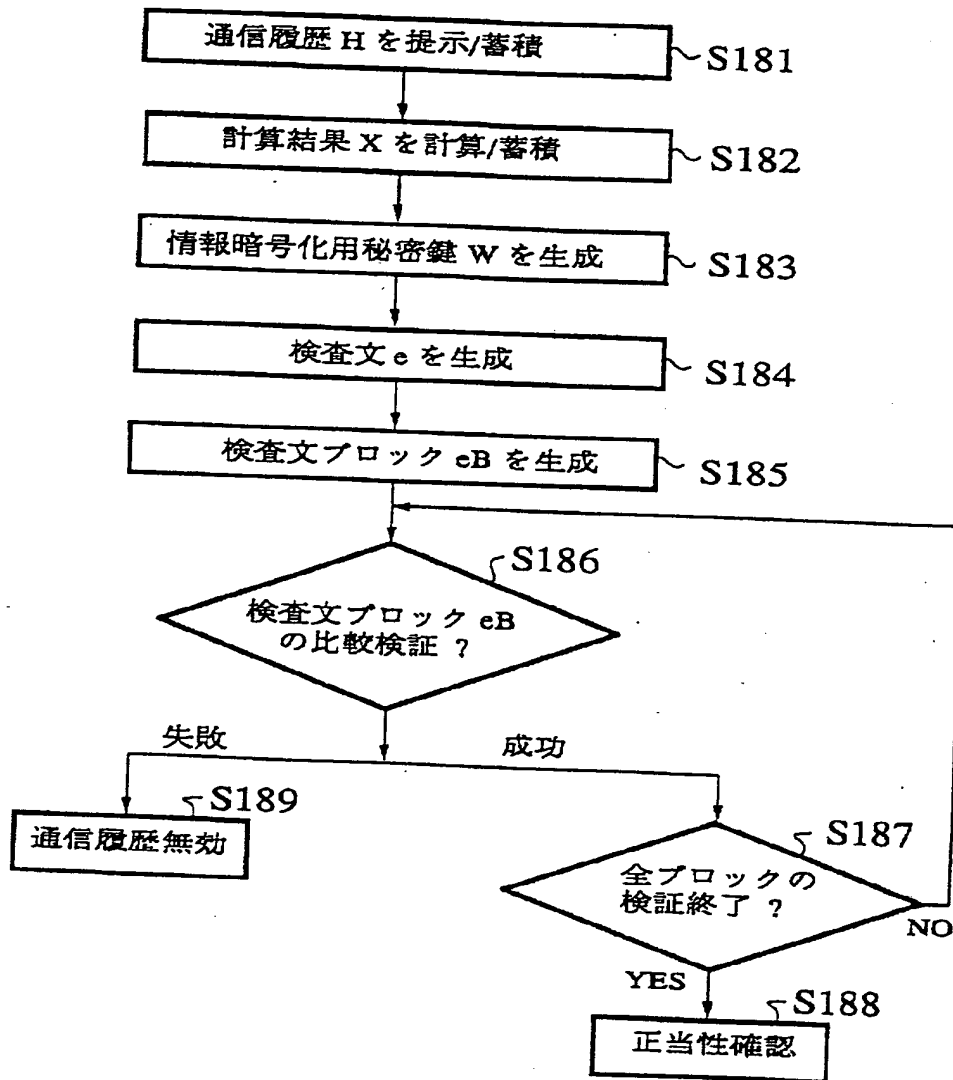
〔図10〕



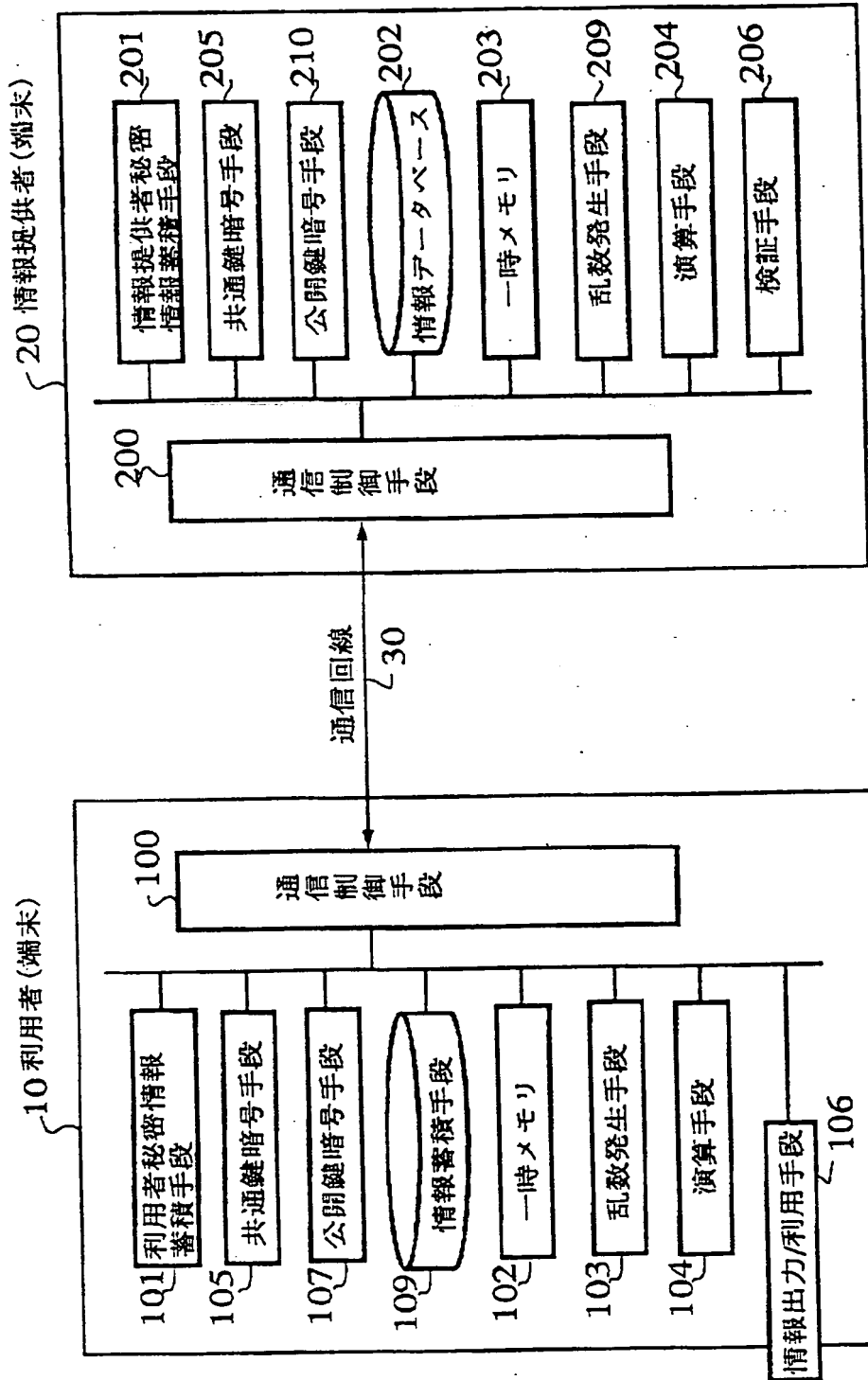
【図11】



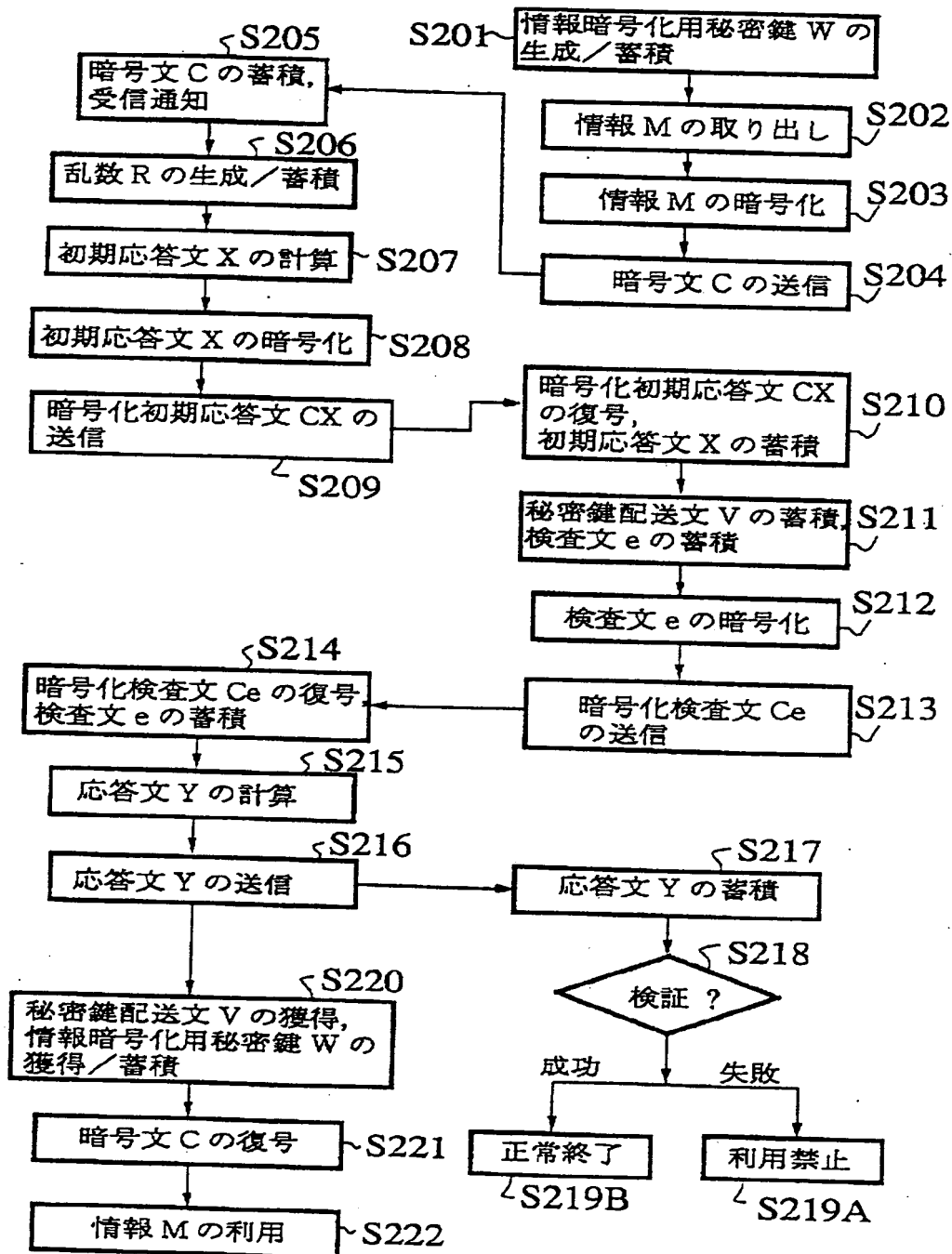
【図 12】



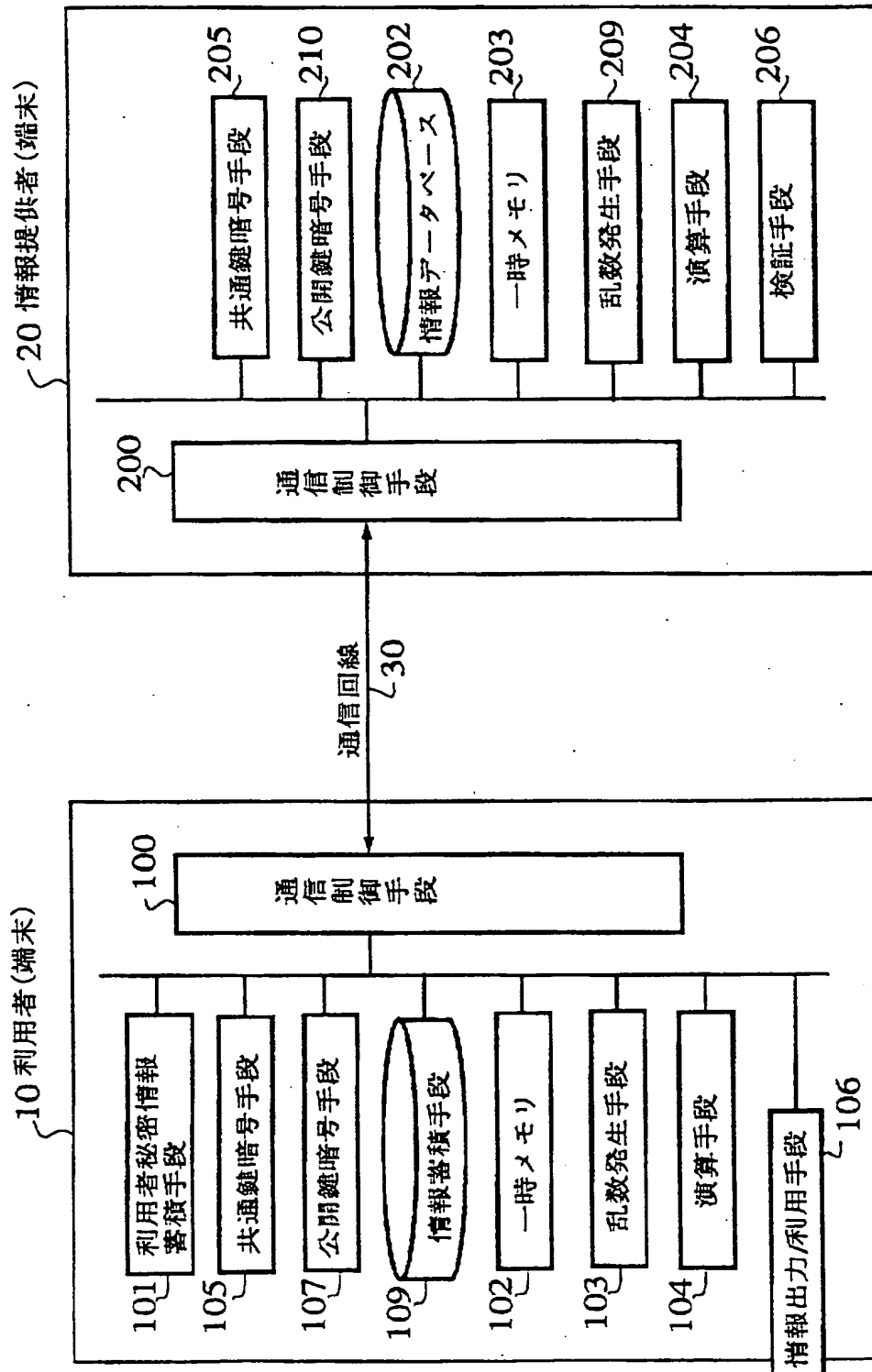
[図 13]



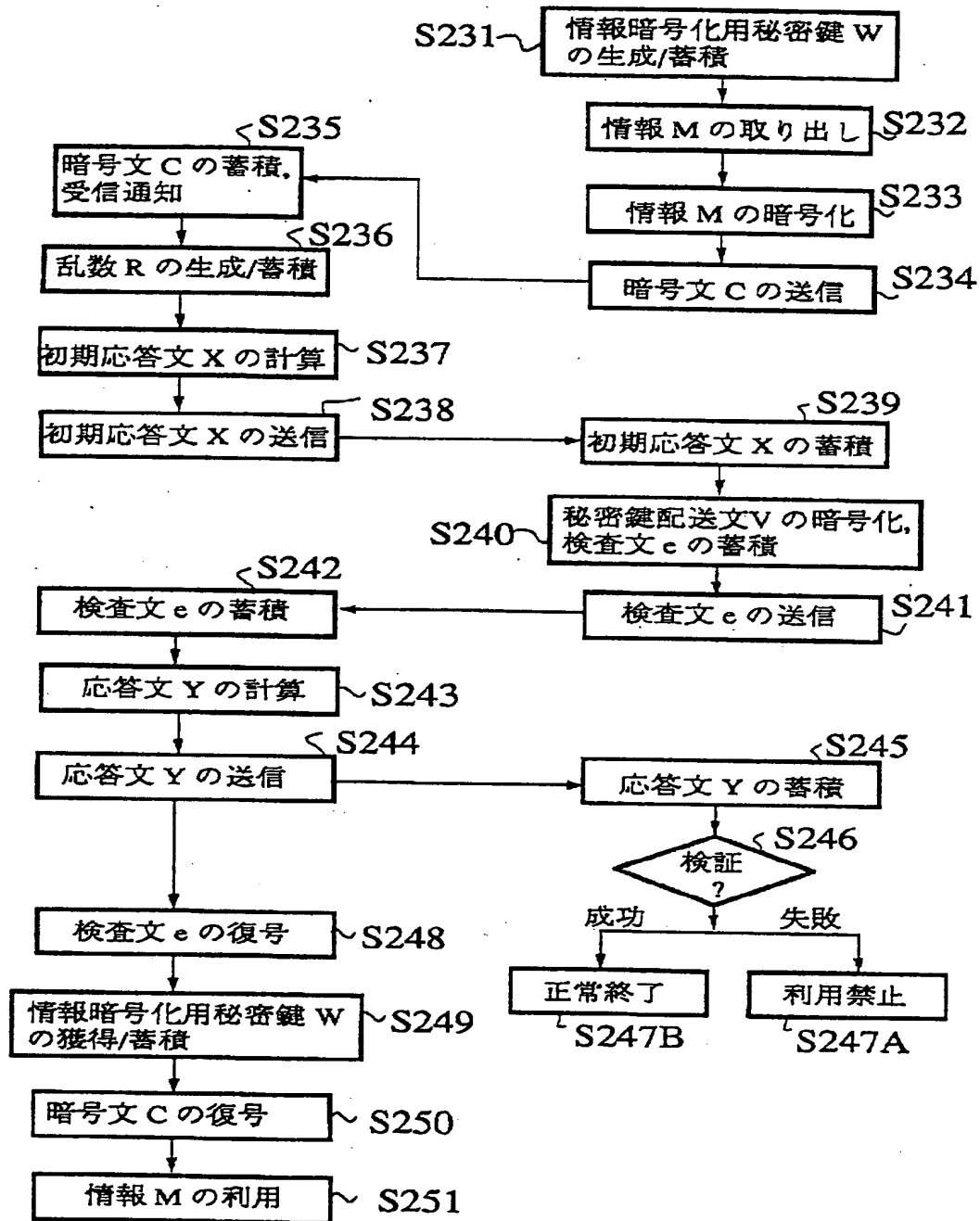
【図 14】



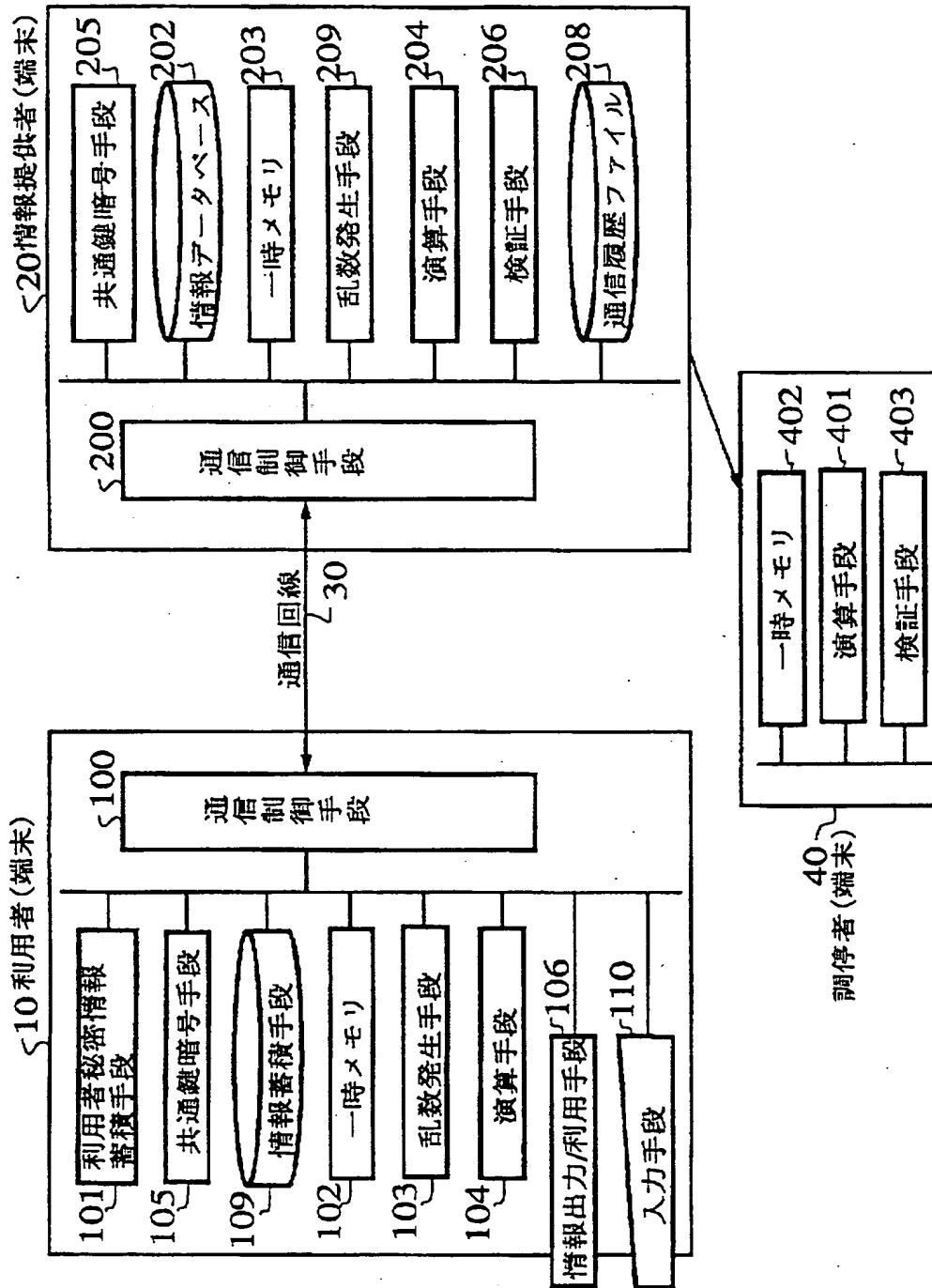
[図15]



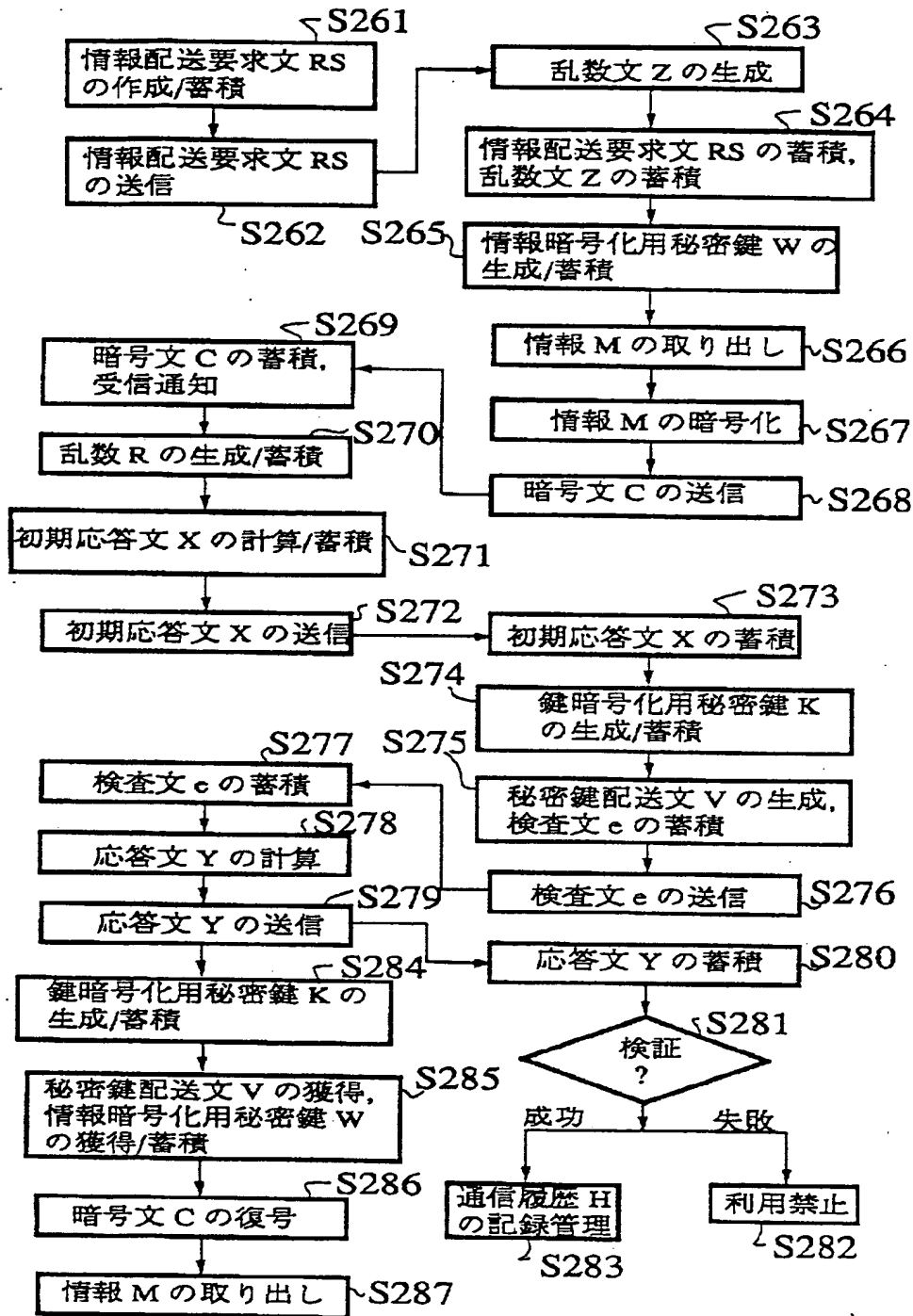
【図 16】



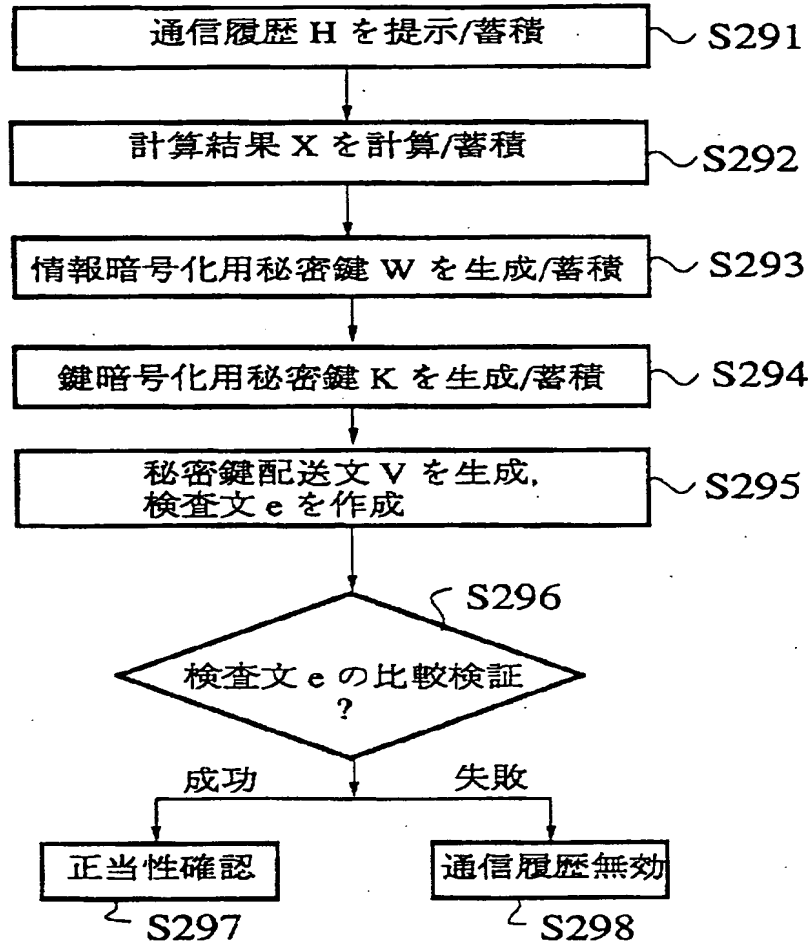
[図 17]



【図18】



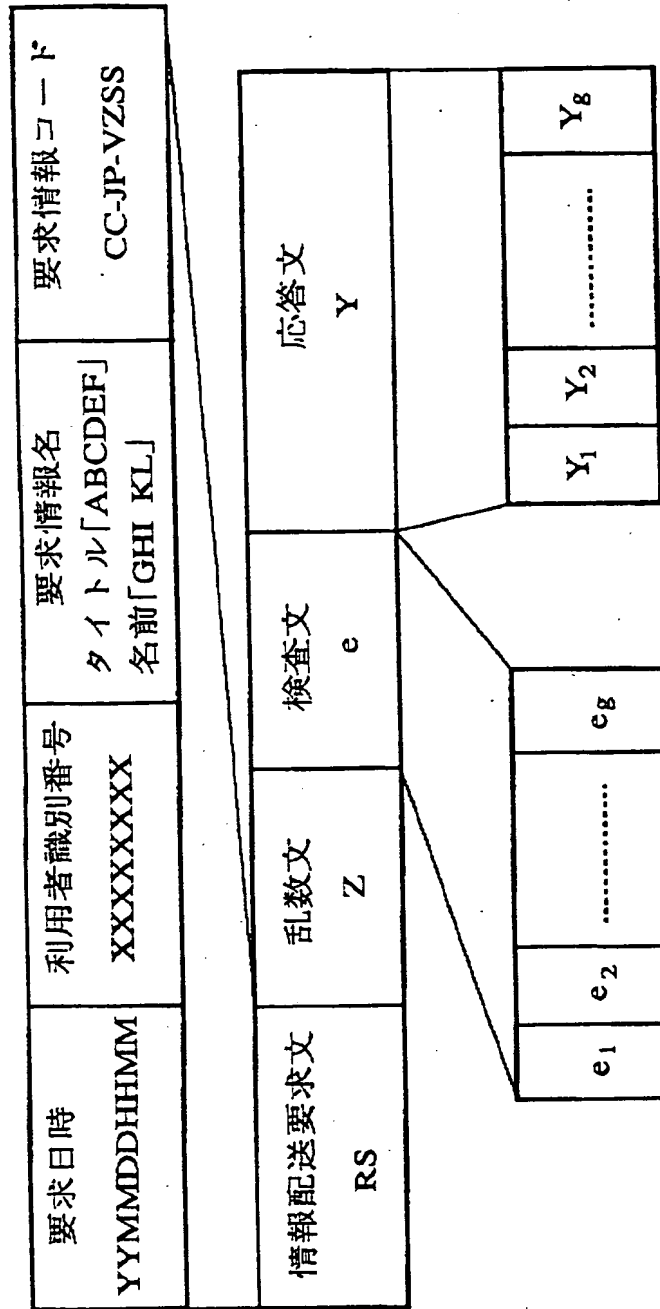
【図19】



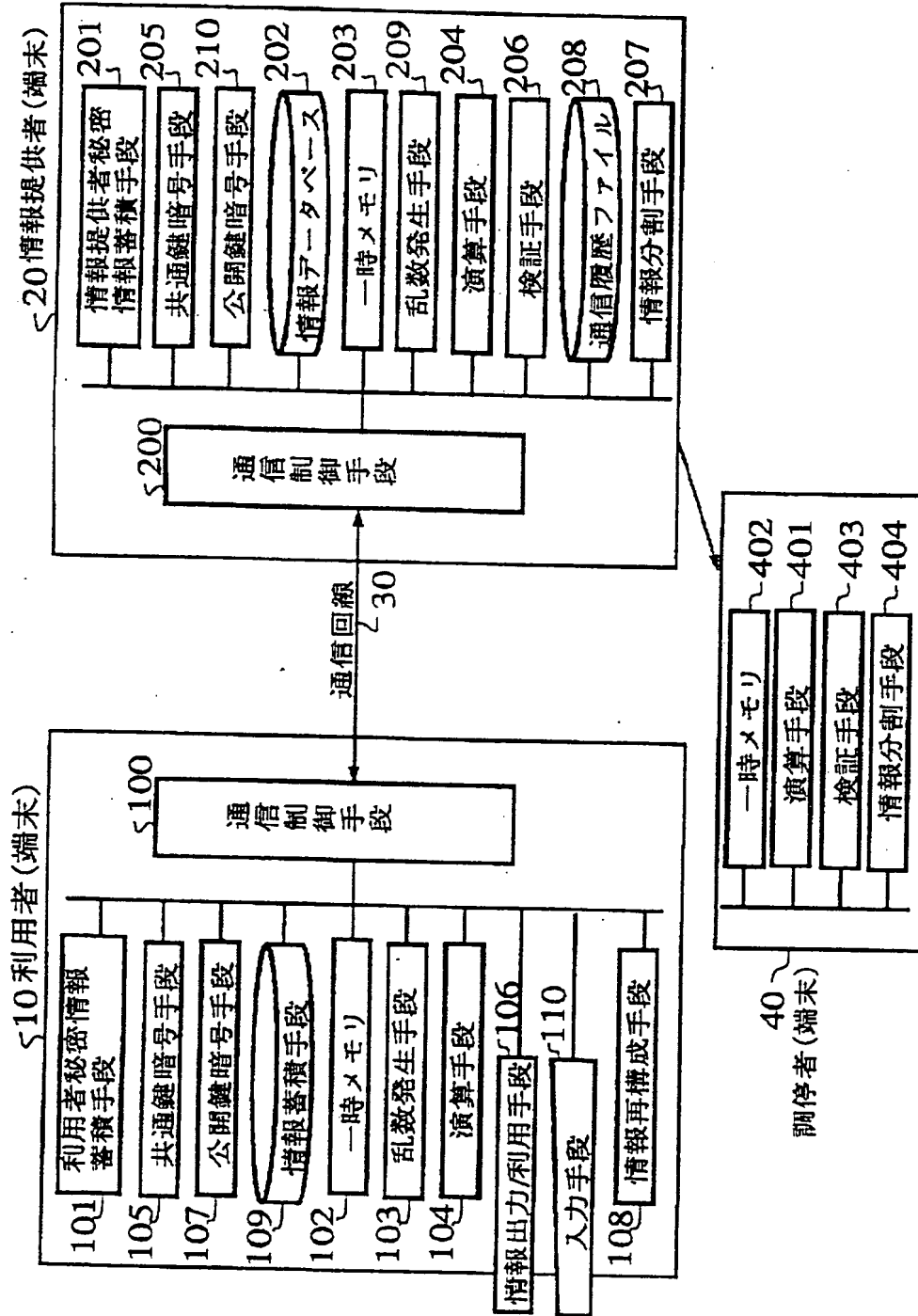
【図 20】

要求日時 YYMMDDHHMM	利用者識別番号 XXXXXXXXXX	要求情報名 タイトル「ABCDEF」 名前「GHI KL」	要求情報コード CC-JP-VZSS
--------------------	-----------------------	-------------------------------------	-----------------------

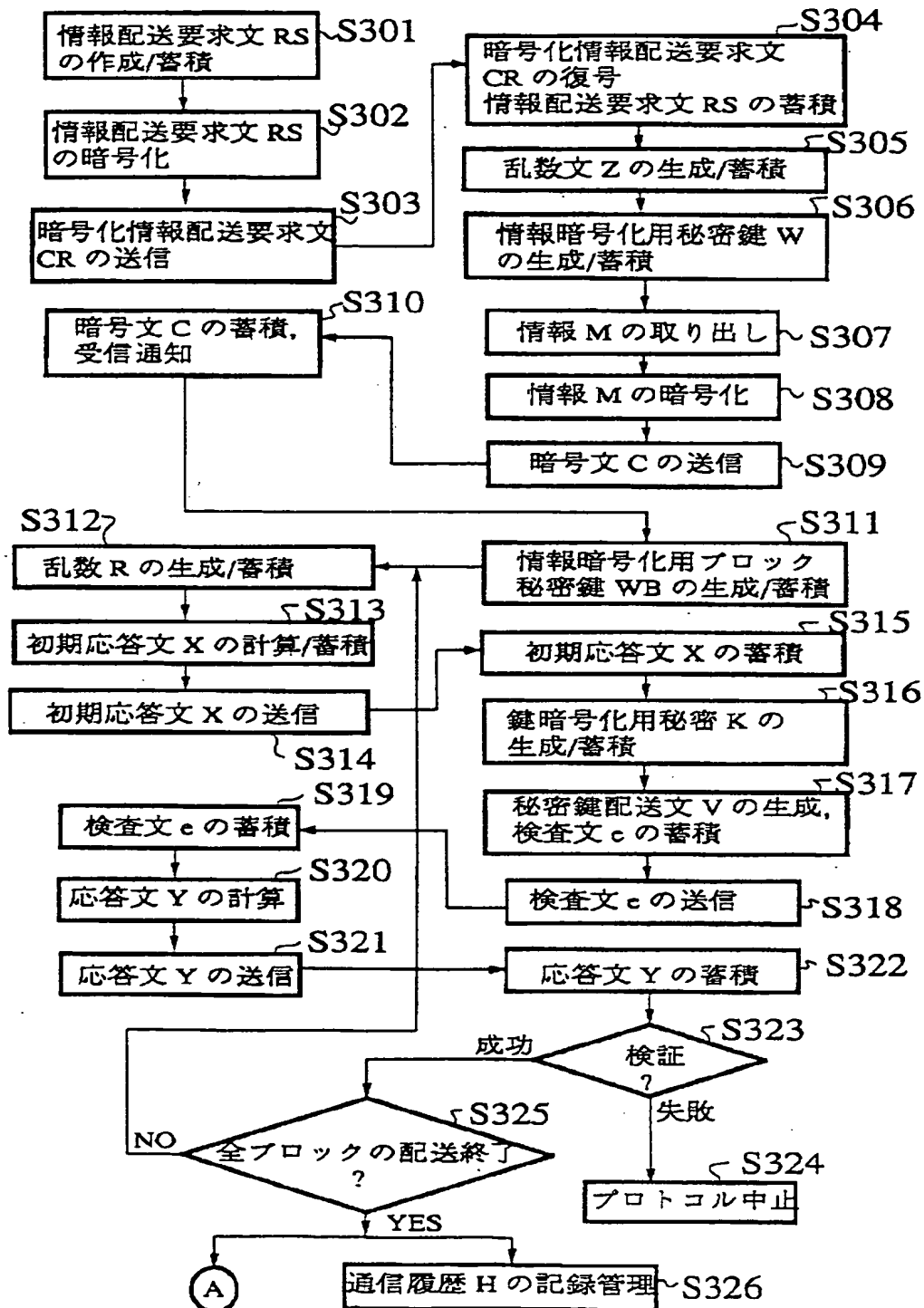
【図 2 1】



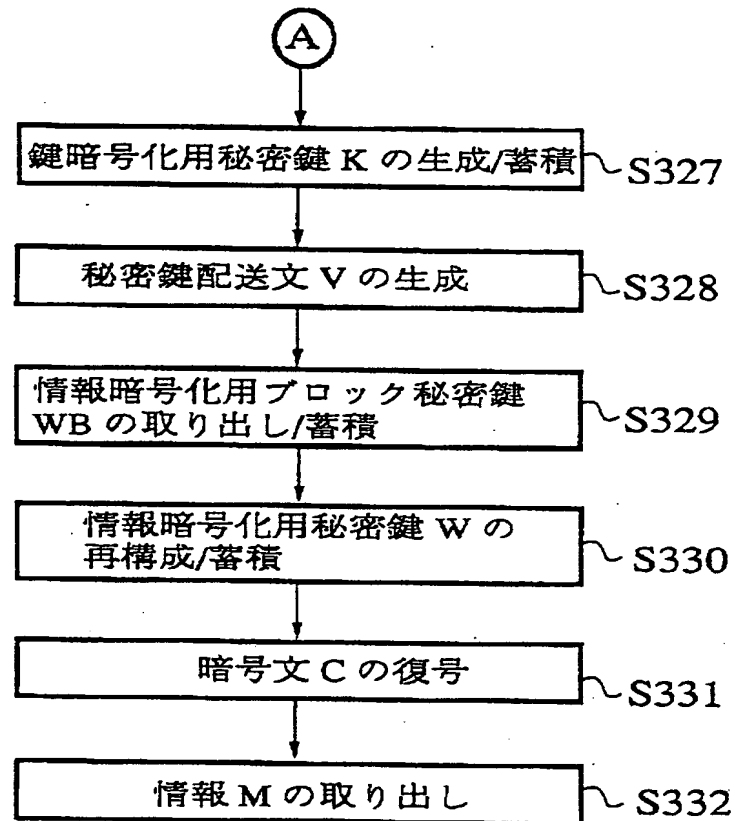
【図 22】



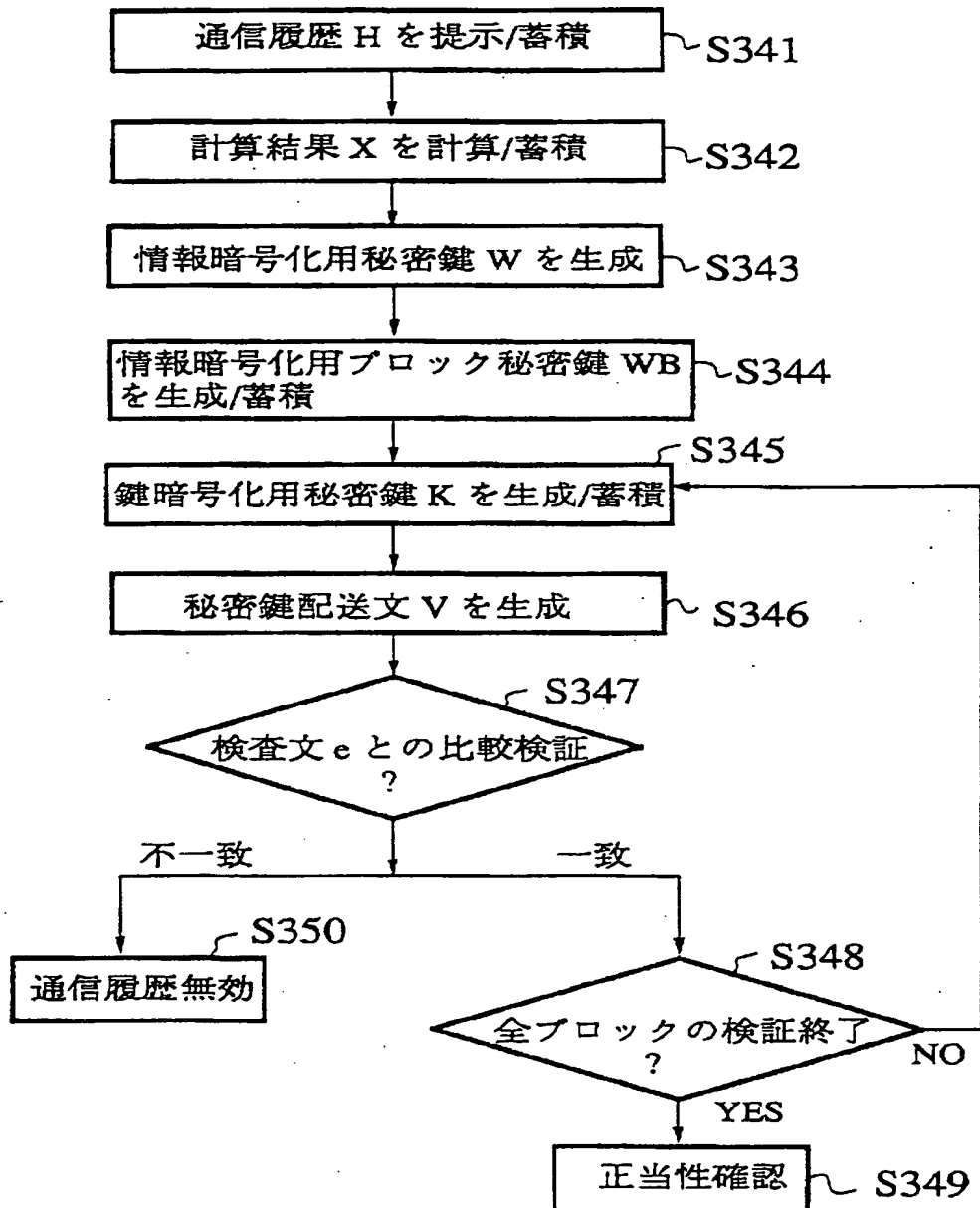
【図23】



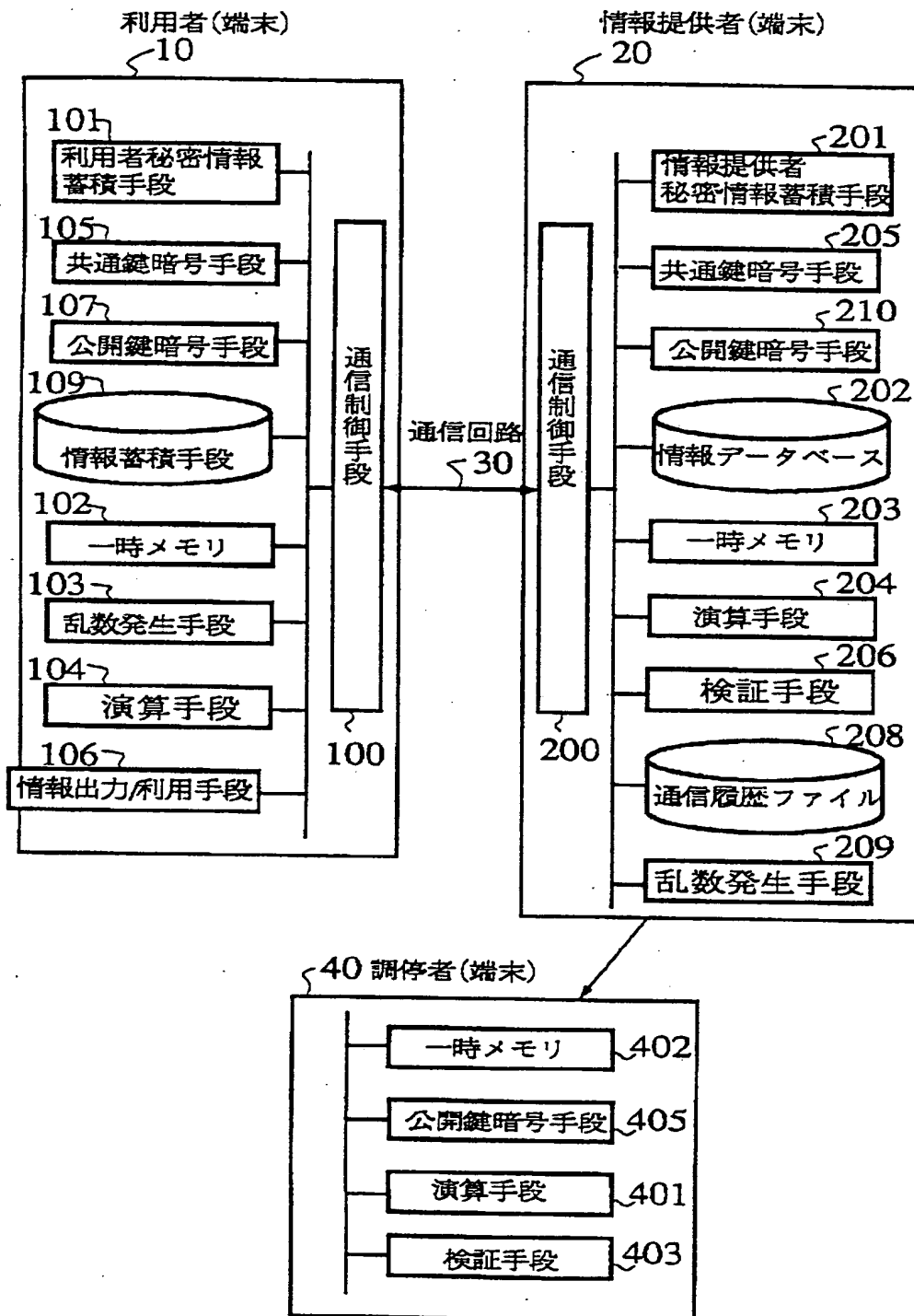
【図 24】



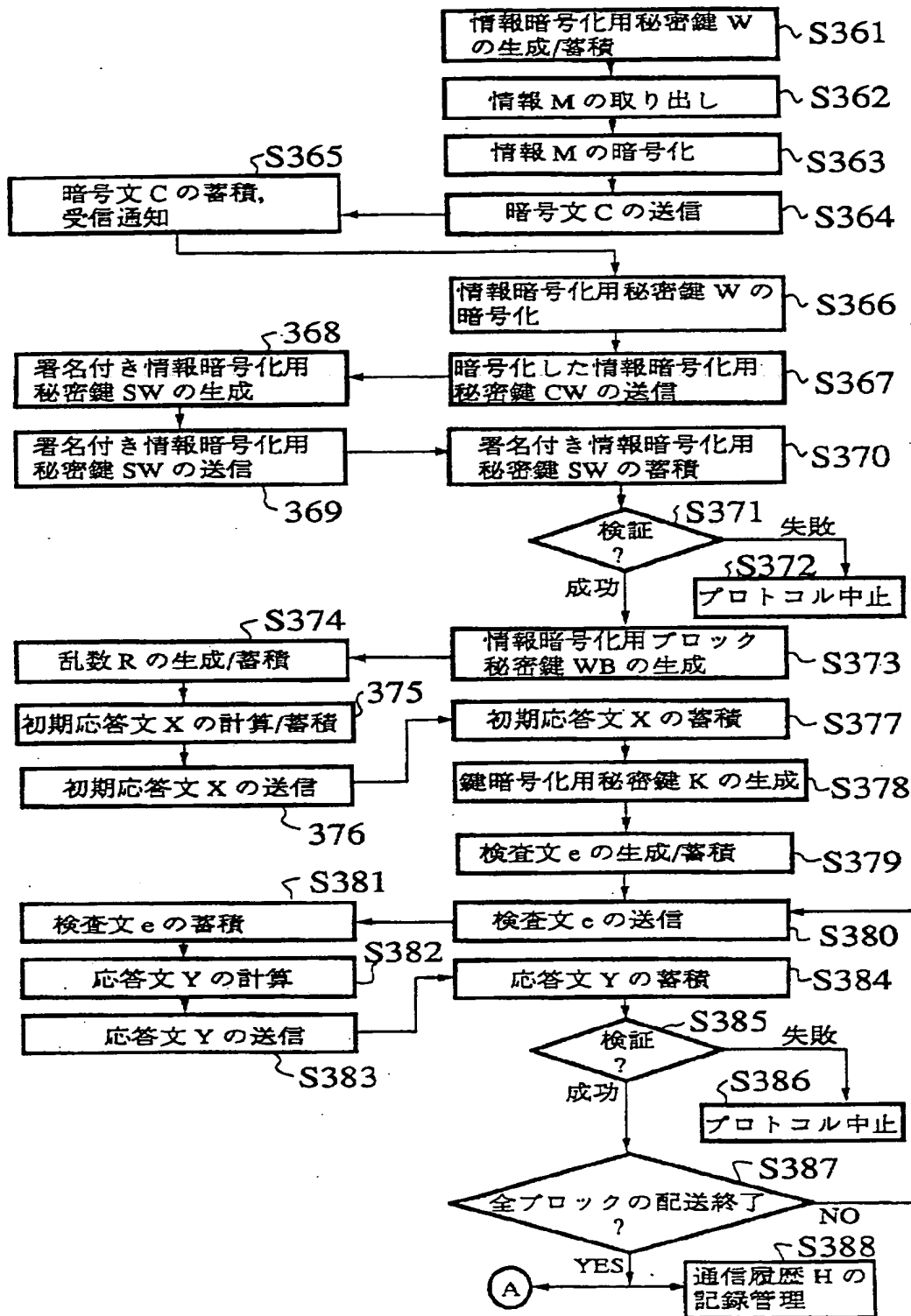
【図25】



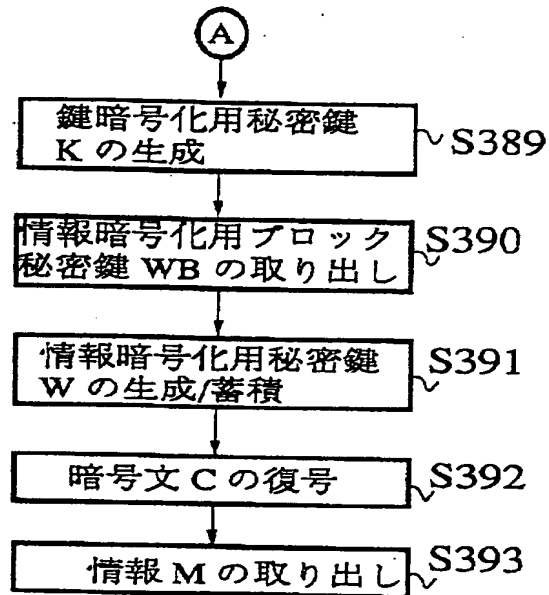
【図26】



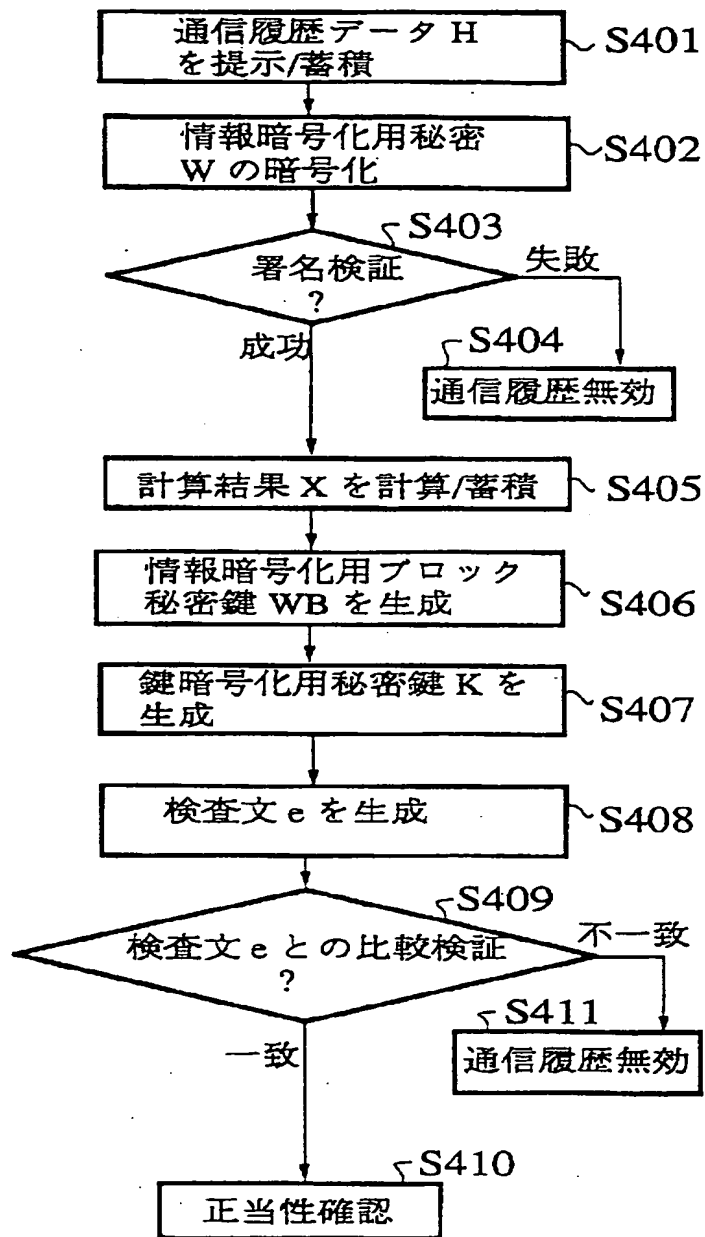
【図 27】



【図 28】



【図 29】



フロントページの続き

(51) Int. Cl. 6

G 0 9 C 1/00

識別記号

庁内整理番号

7259-5 J

F I

技術表示箇所

This Page Blank (uspto)